Coleção SCHAUM

Problema Resolvido

Matemática Discreta

Terceira edição

Mais de 450 problemas resolvidos

- Explicações claras e concisas de todos os conceitos
- Inclui conjuntos, teoria dos grafos, álgebra Booleana, cálculo proposicional, máquinas de Turing e muito mais!

A AJUDA PERFEITA PARA SEUS ESTUDOS!

Seymour Lipschutz e Marc Lipson

SEYMOUR LIPSCHUTZ é docente do Departamento de Matemática da Temple University e lecionou no Polytechnic Institute of Brooklyn. Obteve seu Ph.D. no Courant Institute of Mathematical Sciences da New York University, em 1960. É um dos autores mais prolíficos da Coleção Schaum e escreveu também *Probability*: *Finite Mathematics*, 2.ed.; *Beginning Linear Algebra*; *Set Theory*; *Essential Computer Mathematics* e *Álgebra Linear*, 2.ed. (publicado pela Bookman Editora).

MARC LARS LIPSON é docente do Departamento de Matemática da University of Virginia e lecionou na University of Georgia. Obteve seu Ph.D. em finanças na University of Michigan, em 1994. É também coautor com Seymour Lipschutz de *2000 Solved Problems in Discrete Mathematics* e de *Álgebra Linear*, 3.ed. (publicado pela Bookman Editora).

L767m Lipschutz, Seymour.
Matemática discreta [recurso eletrônico] / Seymour Lipschutz, Marc Lars Lipson ; tradução técnica: Adonai Schlup Sant'anna. – 3. ed. – Dados eletrônicos. – Porto Alegre : Bookman, 2013.
(Coleção Schaum)

Editado também como livro impresso em 2013.
ISBN 978-85-65837-78-1

1. Matemática. 2. Matemática discreta. I. Lipson, Marc Lars. II. Título.

CDU 51

Catalogação na publicação: Ana Paula M. Magnus – CRB 10/2052

Seymour Lipschutz
Temple University

Marc Lars Lipson
University of Virginia

Matemática Discreta

Terceira edição

Tradutor técnico
Adonai Schlup Sant'anna
Pós-Doutorado em Física Teórica pela Stanford University – EUA
Professor Associado do Departamento de Matemática da Universidade Federal do Paraná (UFPR)

Versão impressa
desta obra: 2013

2013

Obra originalmente publicada sob o título
Schaum's Outline for Discrete Mathematics, 3rd Edition.
ISBN 0071615865 / 9780071615860

Gerente Editorial: *Arysinha Jacques Affonso*

Colaboraram nesta edição:

Editora: *Maria Eduarda Fett Tabajara*

Capa: *VS Digital* (arte sobre capa original)

Leitura final: *Miriam Cristina Flores*

Editoração: *Techbooks*

BOOKMAN EDITORA LTDA., uma empresa do GRUPO A EDUCAÇÃO S.A.
Av. Jerônimo de Ornelas, 670 – Santana
90040-340 – Porto Alegre – RS
Fone: (51) 3027-7000 Fax: (51) 3027-7070

Unidade São Paulo
Av. Embaixador Macedo Soares, 10.735 – Pavilhão 5 – Cond. Espace Center
Vila Anastácio – 05095-035 – São Paulo – SP
Fone: (11) 3665-1100 Fax: (11) 3667-1333

SAC 0800 703-3444 – www.grupoa.com.br

IMPRESSO NO BRASIL
PRINTED IN BRAZIL

Prefácio

Matemática discreta, o estudo de sistemas finitos, tem se tornado cada vez mais importante à medida que a era do computador avança. O computador digital é basicamente uma estrutura finita, e muitas de suas propriedades podem ser entendidas e interpretadas no escopo de sistemas matemáticos finitos. Por apresentar o conteúdo mais essencial, este livro pode ser empregado como referência principal em uma disciplina regular de matemática discreta ou como complemento para os demais livros-texto correntemente em uso.

Os três primeiros capítulos cobrem o conteúdo padrão sobre conjuntos, relações, funções e algoritmos. Em seguida, há capítulos sobre lógica, contagem e probabilidade. Temos ainda três capítulos sobre teoria dos grafos: grafos, grafos orientados e árvores binárias. Por fim, três capítulos individuais sobre propriedades dos inteiros, linguagens, máquinas, conjuntos ordenados e reticulados, álgebra Booleana, bem como apêndices sobre vetores e matrizes, e sistemas algébricos. O capítulo referente a funções e algoritmos inclui uma discussão sobre cardinalidade e conjuntos contáveis e complexidade. Os capítulos sobre teoria dos grafos trazem discussões sobre planaridade, transversabilidade, caminhos mínimos e algoritmos de Warshall e Huffman. Enfatizamos que os capítulos foram escritos de modo que a ordem possa ser mudada sem dificuldade ou perda de continuidade.

Cada capítulo começa com uma clara qualificação de definições pertinentes, princípios e teoremas com material ilustrativo e descritivo. Isso é acompanhado por listas de problemas resolvidos e complementares. Os problemas resolvidos servem para ilustrar e ampliar o assunto, e também incluem demonstrações de teoremas. Os problemas complementares oferecem uma revisão completa do tema do capítulo. O material vai além do que possa ser abordado na maioria dos cursos. Isso foi feito para tornar o livro mais flexível, oferecer um texto de referência mais útil e estimular interesse mais avançado nos tópicos.

Gostaríamos de agradecer à equipe da Coleção Schaum da McGraw-Hill pelas valiosas sugestões e pela proveitosa colaboração. Agradecemos também a Michel Falus por sua cuidadosa revisão do manuscrito. Por fim, o Professor Lipschutz expressa sua gratidão ao seu mentor, orientador e amigo, William Magnus, o qual o apresentou a beleza da matemática.

Seymour Lipschutz
Marc Lars Lipson

Sumário

Teoria de Conjuntos

1.1 INTRODUÇÃO

O conceito de *conjunto* aparece em toda a matemática. Este capítulo introduz a notação e a terminologia básicas da teoria de conjuntos usadas ao longo deste livro. O capítulo encerra com a definição formal de indução matemática e exemplos.

1.2 CONJUNTOS E ELEMENTOS, SUBCONJUNTOS

Um *conjunto* pode ser entendido como qualquer coleção bem definida de objetos, conhecidos como os *elementos* ou *membros* do conjunto. Geralmente se empregam letras maiúsculas $A, B, X, Y, \ldots$, para denotar conjuntos, e letras minúsculas, $a, b, x, y, \ldots$, para denotar elementos de conjuntos.† Sinônimos para "conjunto" são "classe", "coleção" e "família".

Pertinência em um conjunto é denotada como segue:

$a \in S$ denota que a pertence a um conjunto S
$a, b \in S$ denota que a e b pertencem a um conjunto S

Aqui, $\in$ é o símbolo que significa "é um elemento de". Empregamos $\notin$ para dizer "não é um elemento de".

Especificando conjuntos

Há essencialmente duas maneiras para especificar um conjunto em particular. Uma delas, se possível, é listar seus elementos separados por vírgulas e contidos entre chaves { }. Uma segunda maneira é estabelecer as propriedades que caracterizam os elementos no conjunto. Exemplos ilustrando essas duas notações são:

$$A = \{1, 3, 5, 7, 9\} \text{ e } B = \{x \mid x \text{ é um inteiro par}, x > 0\}$$

Ou seja, A consiste nos números 1, 3, 5, 7, 9. O segundo conjunto, o qual se lê

B é o conjunto dos x tal que cada x é um inteiro par e x é maior do que 0,

corresponde ao conjunto B cujos elementos são os inteiros pares positivos. Observe que uma letra, geralmente x, é usada para denotar um elemento típico do conjunto, a linha vertical | se lê como "tal que" e a vírgula se lê como "e".

Exemplo 1.1

(a) O conjunto A acima também pode ser escrito como $A = \{x \mid x \text{ é um inteiro positivo ímpar}, x < 10\}$

---

† N. de T.: Esta notação dos autores pode parecer confusa para o leitor, pois nada impede que um conjunto tenha como elementos outros conjuntos.

(b) Não podemos listar todos os elementos do conjunto B recém-dado, apesar de frequentemente especificarmos tal conjunto como

$$B = \{2, 4, 6, \ldots\}$$

onde assumimos que todo mundo sabe o que queremos dizer. Observe que $8 \in B$, mas $3 \notin B$

(c) Sejam $E = \{x \mid x^2 - 3x + 2 = 0\}$, $F = \{2, 1\}$ e $G = \{1, 2, 2, 1\}$. Então $E = F = G$.

Enfatizamos que um conjunto não depende da maneira como seus elementos são colocados. Um conjunto permanece o mesmo se seus elementos são repetidos ou rearranjados.

Mesmo que possamos listar os elementos de um conjunto, isso pode não ser prático. Ou seja, descrevemos um conjunto listando seus elementos somente se o conjunto contém poucos membros; caso contrário, descrevemos um conjunto pela propriedade que caracteriza seus elementos.

Subconjuntos

Suponha que todo elemento de um conjunto A é também elemento de um conjunto B, ou seja, suponha que $a \in A$ implique $a \in B$. Então A é dito um subconjunto de B. Também dizemos que A está contido em B ou que B contém A. Esta relação é escrita

$$A \subseteq B \text{ ou } B \supseteq A$$

Dois conjuntos são iguais se ambos têm os mesmos elementos ou, equivalentemente, se cada conjunto está contido no outro. Ou seja,

$$\boxed{A = B \text{ se, e somente se, } A \subseteq B \text{ e } B \subseteq A}$$

Se A não é subconjunto de B, isto é, se pelo menos um elemento de A não pertence a B, escrevemos $A \not\subseteq B$.

Exemplo 1.2 Considere os conjuntos

$$A = \{1, 3, 4, 7, 8, 9\}, \quad B = \{1, 2, 3, 4, 5\}, \quad C = \{1, 3\}.$$

Então $C \subseteq A$ e $C \subseteq B$, uma vez que 1 e 3, os elementos de C, também são membros de A e B. Mas $B \not\subseteq A$, pois alguns dos elementos de B, por exemplo, 2 e 5, não pertencem a A. Analogamente, $A \not\subseteq B$.

Propriedade 1: É prática comum em matemática colocar uma barra vertical "|" ou uma barra "/" sobreposta a um símbolo para indicar o significado oposto ou negativo do símbolo.

Propriedade 2: A sentença $A \subseteq B$ não exclui a possibilidade de $A = B$. De fato, para cada conjunto A temos $A \subseteq A$, uma vez que, trivialmente, todo elemento de A pertence a A. Contudo, se $A \subseteq B$ e $A \neq B$, então dizemos que A é um subconjunto próprio de B (às vezes escrito como $A \subset B$).

Propriedade 3: Suponha que todo elemento de um conjunto A pertença a um conjunto B e todo elemento de B pertença a um conjunto C. Então, claramente, cada elemento de A também pertence a C. Em outras palavras, se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

As observações acima implicam o seguinte teorema.

Teorema 1.1: Sejam A, B e C conjuntos quaisquer. Então:

(i) $A \subseteq A$

(ii) Se $A \subseteq B$ e $B \subseteq A$, então $A = B$

(iii) Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$

Símbolos especiais

Diversos conjuntos ocorrem muito frequentemente no texto, e usamos símbolos especiais para eles. Alguns desses símbolos são:

N = o conjunto dos números naturais ou inteiros positivos: 1, 2, 3, ...

$\mathbf{Z}$ = o conjuntos de todos os inteiros: . . . , −2, −1, 0, 1, 2, . . .
$\mathbf{Q}$ = o conjunto dos números racionais
$\mathbf{R}$ = o conjunto dos números reais
$\mathbf{C}$ = o conjunto dos números complexos

Observe que $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$.

Conjunto universo, conjunto vazio

Todos os conjuntos sob investigação em qualquer aplicação da teoria de conjuntos são considerados como membros de um grande conjunto fixo chamado de *conjunto universo*, o qual denotamos por

$$\mathbf{U}$$

a não ser que algo contrário seja estabelecido ou inferido.

Dados um conjunto universo $\mathbf{U}$ e uma propriedade P, pode não haver qualquer elemento de $\mathbf{U}$ que tenha a propriedade P. Por exemplo, o conjunto a seguir não tem elementos.

$$S = \{x \mid x \text{ é um inteiro positivo}, x^2 = 3\}$$

Tal conjunto sem elementos é chamado de *conjunto vazio* ou *conjunto nulo* e é denotado por

$$\emptyset$$

Existe um único conjunto vazio. Ou seja, se S e T são ambos vazios, então $S = T$, uma vez que eles têm exatamente os mesmos elementos, a saber, nenhum.

O conjunto vazio $\emptyset$ é também subconjunto de qualquer conjunto. Assim, temos o seguinte resultado simples que escrevemos formalmente como.

Teorema 1.2: Para qualquer conjunto A, temos $\emptyset \subseteq A \subseteq \mathbf{U}$.

Conjuntos disjuntos

Dois conjuntos A e B são chamados de *disjuntos* se eles não têm elemento algum em comum. Por exemplo, suponha que

$$A = \{1, 2\}, \quad B = \{4, 5, 6\} \quad \text{e} \quad C = \{5, 6, 7, 8\}$$

Então A e B são disjuntos, e A e C são disjuntos. Mas B e C não são disjuntos, pois B e C têm elementos em comum, por exemplo, 5 e 6. Observamos que se A e B são disjuntos, então nenhum deles é subconjunto do outro (a menos que um seja o conjunto vazio).

1.3 DIAGRAMAS DE VENN

Um diagrama de Venn é uma representação pictórica de conjuntos na qual conjuntos são representados por áreas delimitadas no plano. O conjunto universal $\mathbf{U}$ é representado pelo interior de um retângulo, e os outros conjuntos são representados por discos dentro do retângulo. Se $A \subseteq B$, então o disco representando A está completamente dentro do disco representando B, como na Fig. 1-1(*a*). Se A e B são disjuntos, então o disco representando A é separado do disco representando B, como na Fig. 1-1(*b*).

(*a*) $A \subseteq B$ (*b*) A e B são disjuntos (*c*)

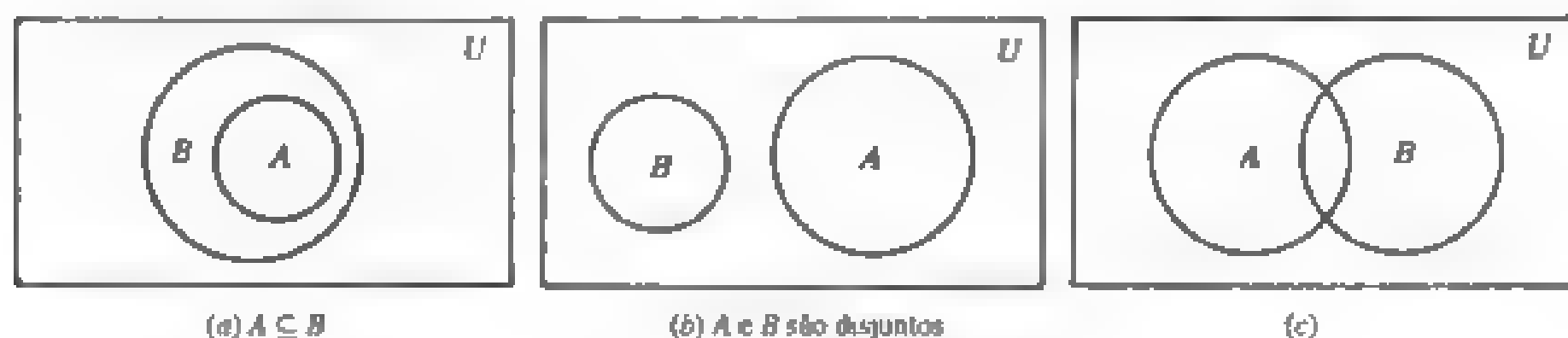



Figura 1-1

No entanto, se A e B são dois conjuntos arbitrários, é possível que alguns objetos estejam em A, mas não em B, alguns em B, mas não em A, alguns em ambos, ou alguns nem em A, nem em B, portanto, no caso geral, representamos A e B como na Fig. 1-1(c).

Argumentos e diagramas de Venn

Muitas afirmações verbais são essencialmente declarações sobre conjuntos e, portanto, podem ser descritas por diagramas de Venn. Assim, por vezes, diagramas de Venn podem ser usados para determinar se um argumento é válido ou não.

Exemplo 1.3 Mostre que o argumento a seguir (adaptado de um livro de lógica de Lewis Carroll, o autor de *Alice no País das Maravilhas*) é válido:

S_1: Todos os meus objetos de lata são frascos de molho.
S_2: Considero todos os seus presentes muito úteis.
S_3: Nenhum dos meus frascos de molho é útil.

S: Seus presentes dados a mim não são feitos de lata.

As afirmações S_1, S_2 e S_3 acima da linha horizontal denotam as premissas, e a afirmação S abaixo da linha denota a conclusão. O argumento é válido se a conclusão S segue logicamente das premissas S_1, S_2 e S_3.

De acordo com S_1, os objetos de lata estão contidos no conjunto de frascos de molho e, a partir de S_3, o conjunto de frascos de molho e o conjunto de coisas úteis são disjuntos. Além disso, de acordo com S_2, o conjunto de "seus presentes" é um subconjunto da coleção de coisas úteis. Consequentemente, podemos esboçar o diagrama de Venn na Fig. 1-2.

A conclusão é claramente válida pelo diagrama de Venn, pois o conjunto de "seus presentes" é disjunto da coleção de objetos de lata.

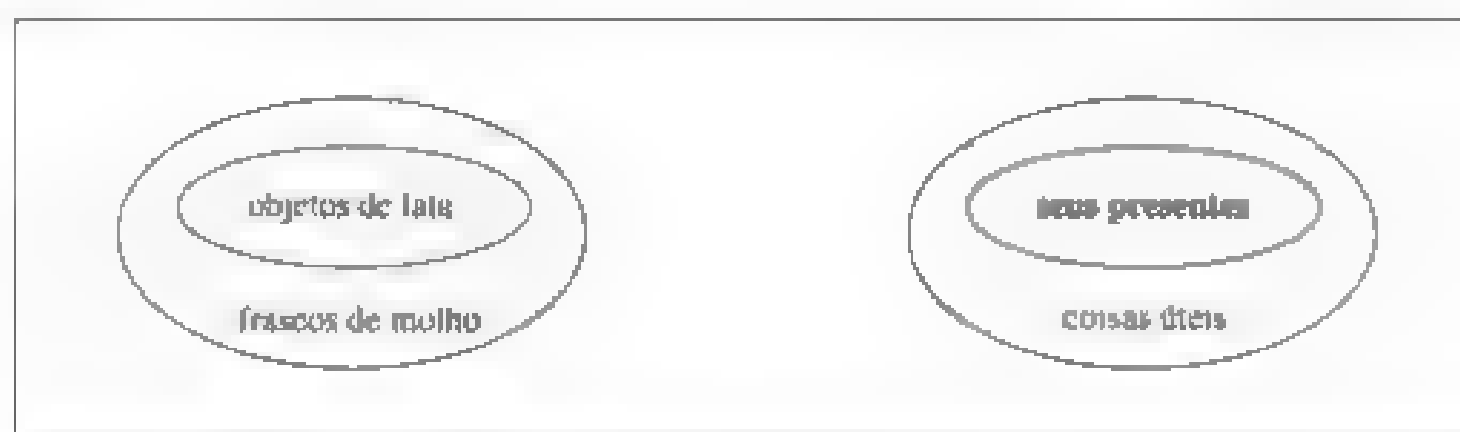



Figura 1-2

1.4 OPERAÇÕES CONJUNTISTAS

Esta seção introduz algumas operações conjuntistas, incluindo as operações básicas de união, interseção e complementar.

União e interseção

A *união* de dois conjuntos A e B, denotada por $A \cup B$, é o conjunto de todos os elementos que pertencem a A ou B, ou seja,

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$$

Aqui, "ou" é usado no sentido de e/ou. A Fig. 1-3(a) é um diagrama de Venn no qual $A \cup B$ é sombreado.

A *interseção* de dois conjuntos A e B, denotada por $A \cap B$, é o conjunto de elementos que pertencem a ambos, A e B, ou seja,

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}$$

A Fig. 1-3(b) é um diagrama de Venn no qual $A \cap B$ é sombreado.

(a) $A \cup B$ está sombreado

(b) $A \cap B$ está sombreado

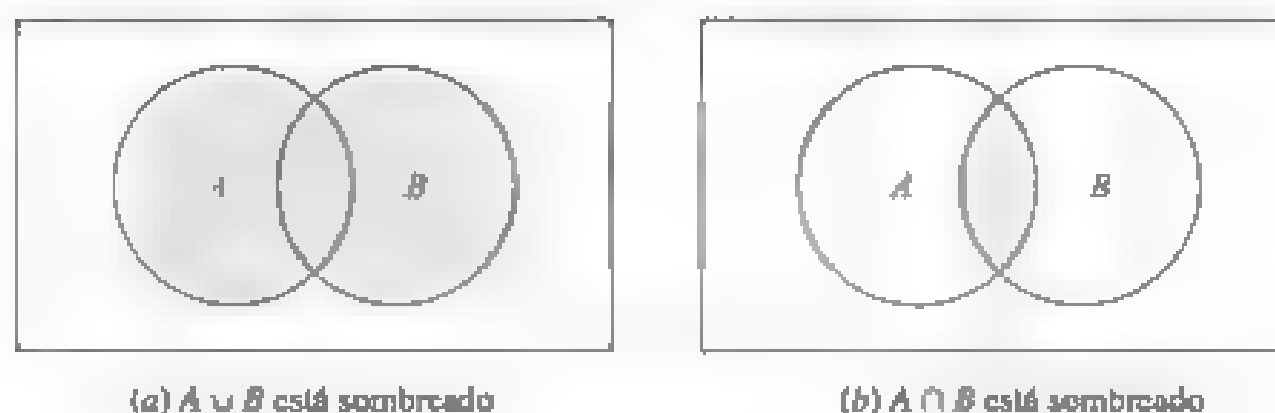



Figura 1-3

Lembre que os conjuntos A e B são ditos *disjuntos* ou *sem interseção* se eles não têm elementos em comum ou, usando a definição de interseção, se $A \cap B = \emptyset$, o conjunto vazio. Suponha que

$$S = A \cup B \quad \text{e} \quad A \cap B = \emptyset$$

Então S é dita a *união disjunta* de A e B.

Exemplo 1.4

(a) Sejam $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$ e $C = \{2, 3, 8, 9\}$. Então

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}, \quad A \cup C = \{1, 2, 3, 4, 8, 9\}, \quad B \cup C = \{2, 3, 4, 5, 6, 7, 8, 9\},$$
$$A \cap B = \{3, 4\}, \quad A \cap C = \{2, 3\}, \quad B \cap C = \{3\}$$

(b) Seja $\mathbf{U}$ o conjunto de estudantes em uma universidade, sendo M o conjunto de estudantes do sexo masculino e F o conjunto de estudantes do sexo feminino. Então $\mathbf{U}$ é a união disjunta de M e F; isto é,

$$\mathbf{U} = M \cup F \quad \text{e} \quad M \cap F = \emptyset$$

Isso decorre do fato de que todo estudante em $\mathbf{U}$ está em M ou F, e claramente nenhum estudante pertence a ambos, M e F, ou seja, M e F são disjuntos.

As propriedades de união e interseção a seguir devem ser observadas.

Propriedade 1: Todo elemento x em $A \cap B$ pertence a ambos, A e B; portanto, x pertence a A e x pertence a B. Assim, $A \cap B$ é um subconjunto de A e de B; ou seja

$$A \cap B \subseteq A \quad \text{e} \quad A \cap B \subseteq B$$

Propriedade 2: Um elemento x pertence à união $A \cup B$ se x pertence a A ou se x pertence a B; logo, todo elemento de A pertence a $A \cup B$, e todo elemento de B pertence a $A \cup B$. Ou seja,

$$A \subseteq A \cup B \quad \text{e} \quad B \subseteq A \cup B$$

Formulamos os resultados acima como:

Teorema 1.3: Para quaisquer conjuntos A e B, temos.

$$\text{(i)}\, A \cap B \subseteq A \subseteq A \cup B \quad \text{e} \quad \text{(ii)}\, A \cap B \subseteq B \subseteq A \cup B.$$

A operação de inclusão conjuntista está intimamente relacionada às operações de união e interseção, como se mostra pelo teorema a seguir.

Teorema 1.4: As fórmulas a seguir são equivalentes: $A \subseteq B$, $\quad A \cap B = A$, $\quad A \cup B = B$

Este teorema é demonstrado no Problema 1.8. Outras condições equivalentes a $A \subseteq B$ são dadas no Problema 1.31.

(a) A^C é sombreado (b) $A \backslash B$ é sombreado (c) $A \oplus B$ é sombreado

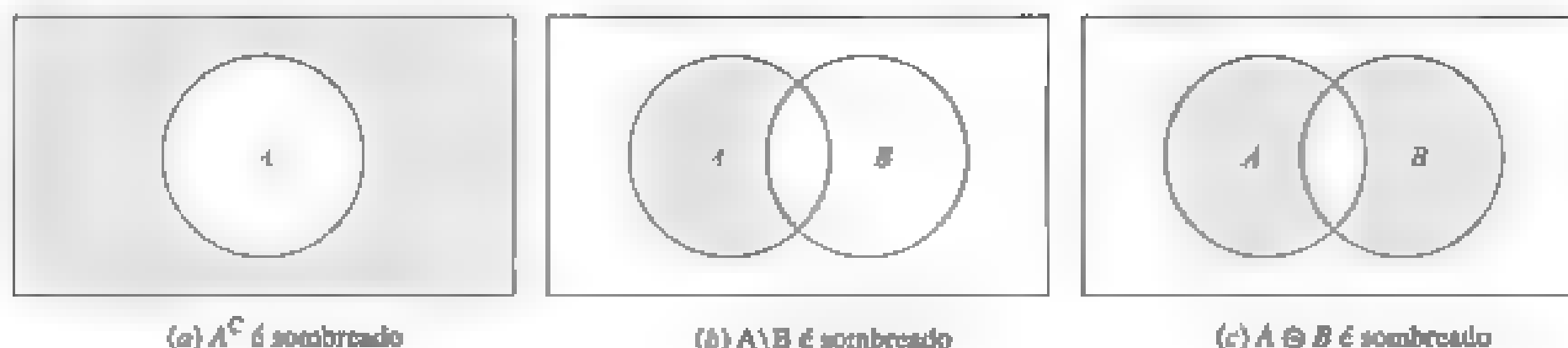



Figura 1-4

Complementares, diferenças, diferenças simétricas

Lembre que todos os conjuntos sob consideração em um dado momento são subconjuntos de um conjunto universo fixo U. O *complementar absoluto* ou, simplesmente, o *complementar* de um conjunto A, denotado por A^C, é o conjunto de elementos que pertencem a U, mas que não pertencem a A. Ou seja,

$$A^C = \{x \mid x \in \mathbf{U}, x \notin A\}$$

Alguns textos denotam o complemento de A por A' ou $\bar{A}$. A Fig. 1-4(a) é um diagrama de Venn no qual A^C é sombreado.

O *complementar relativo* de um conjunto B relativamente a um conjunto A, ou simplesmente a *diferença* de A por B, denotada por $A \backslash B$, é o conjunto de elementos que pertencem a A, mas que não pertencem a B, isto é

$$A \backslash B = \{x \mid x \in A, x \notin B\}$$

O conjunto $A \backslash B$ se lê "A menos B". Muitos textos denotam $A \backslash B$ por $A - B$ ou $A \sim B$. A Fig. 1-4(b) é um diagrama de Venn no qual $A \backslash B$ é sombreado.

A *diferença simétrica* de conjuntos A e B, denotada por $A \oplus B$, consiste naqueles elementos que pertencem a A ou B, mas não a ambos. Ou seja,

$$A \oplus B = (A \cup B) \backslash (A \cap B) \quad \text{ou} \quad A \oplus B = (A \backslash B) \cup (B \backslash A)$$

A Figura 1-4(c) é um diagrama de Venn no qual $A \oplus B$ é sombreado.

Exemplo 1.5 Suponha que $\mathbf{U} = \mathbf{N} = \{1, 2, 3, \ldots\}$ é o conjunto universo. Faça

$A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$, $C = \{2, 3, 8, 9\}$, $E = \{2, 4, 6, \ldots\}$.(Aqui E é o conjunto de inteiros positivos pares.) Então:

$$A^C = \{5, 6, 7, \ldots\}, \quad B^C = \{1, 2, 8, 9, 10, \ldots\}, \quad E^C = \{1, 3, 5, 7, \ldots\}.$$

Ou seja, E^C é o conjunto de inteiros positivos ímpares. Também:

$$A \backslash B = \{1, 2\}, \quad A \backslash C = \{1, 4\}, \quad B \backslash C = \{4, 5, 6, 7\}, \quad A \backslash E = \{1, 3\},$$
$$B \backslash A = \{5, 6, 7\}, \quad C \backslash A = \{8, 9\}, \quad C \backslash B = \{2, 8, 9\}, \quad E \backslash A = \{6, 8, 10, 12, \ldots\}$$

Além disso:

$$A \oplus B = (A \backslash B) \cup (B \backslash A) = \{1, 2, 5, 6, 7\}, \quad B \oplus C = \{2, 4, 5, 6, 7, 8, 9\},$$
$$A \oplus C = (A \backslash C) \cup (C \backslash A) = \{1, 4, 8, 9\}, \quad A \oplus E = \{1, 3, 6, 8, 10, \ldots\}$$

Produtos fundamentais

Considere n conjuntos distintos $A_1, A_2, \ldots, A_n$. Um *produto fundamental* dos conjuntos é um conjunto da forma

$$A_1^* \cap A_2^* \cap \ldots \cap A_n^* \quad \text{onde} \quad A_i^* = A \text{ ou } A_i^* = A^C$$

Observamos que

(i) Existem $m = 2^n$ produtos fundamentais.

(ii) Quaisquer dois produtos fundamentais são disjuntos.

(iii) O conjunto universo **U** é a união de todos os produtos fundamentais.

Assim, U é a união disjunta dos produtos fundamentais (Problema 1.60). Há uma descrição geométrica desses conjuntos, a qual é ilustrada abaixo.

Exemplo 1.6 A Fig. 1-5(a) é o diagrama de Venn de três conjuntos A, B, C. Os $m = 2^3 = 8$ produtos fundamentais dos conjuntos A, B, C são os seguintes:

$$P_1 = A \cap B \cap C, \quad P_3 = A \cap B^C \cap C, \quad P_5 = A^C \cap B \cap C, \quad P_7 = A^C \cap B^C \cap C,$$
$$P_2 = A \cap B \cap C^C, \quad P_4 = A \cap B^C \cap C^C, \quad P_6 = A^C \cap B \cap C^C, \quad P_8 = A^C \cap B^C \cap C^C.$$

Os oito produtos correspondem precisamente às oito regiões disjuntas no diagrama de Venn dos conjuntos A, B, C, como indicado pelos rótulos das regiões na Fig. 1-5 (b).

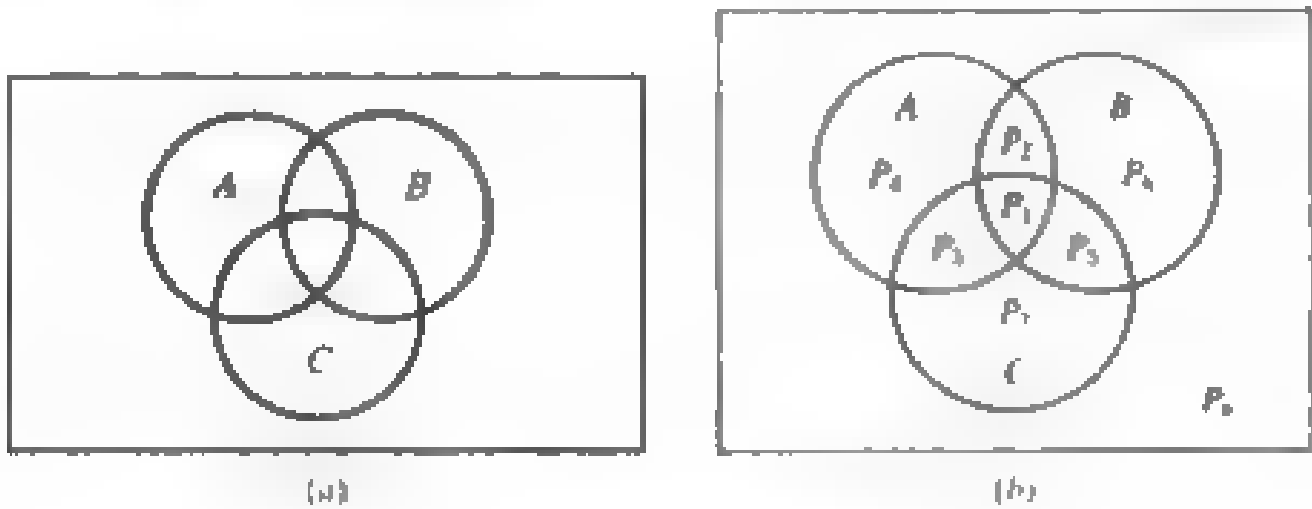



Figura 1-5

1.5 ÁLGEBRA DE CONJUNTOS, DUALIDADE

Conjuntos sob operações de união, interseção e complementar satisfazem a várias leis (identidades) que são listadas na Tabela 1-1. De fato, estabelecemos isso formalmente como:

Teorema 1.5: Conjuntos satisfazem as leis da Tabela 1-1.

Tabela 1-1 Leis da álgebra de conjuntos

Leis da idempotência	(1a) $A \cup A = A$	(1b) $A \cap A = A$
Leis associativas	(2a) $(A \cup B) \cup C = A \cup (B \cup C)$	(2b) $(A \cap B) \cap C = A \cap (B \cap C)$
Leis comutativas	(3a) $A \cup B = B \cup A$	(3b) $A \cap B = B \cap A$
Leis distributivas	(4a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(4b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Leis de identidade	(5a) $A \cup \emptyset = A$	(5b) $A \cap \mathbf{U} = A$
	(6a) $A \cup \mathbf{U} = \mathbf{U}$	(6b) $A \cap \emptyset = \emptyset$
Leis de involução	(7) $(A^C)^C = A$	
Leis de complementos	(8a) $A \cup A^C = \mathbf{U}$	(8b) $A \cap A^C = \emptyset$
	(9a) $\mathbf{U}^C = \emptyset$	(9b) $\emptyset^C = \mathbf{U}$
Leis de DeMorgan	(10a) $(A \cup B)^C = A^C \cap B^C$	(10b) $(A \cap B)^C = A^C \cup B^C$

Observação: Cada lei na Tabela 1-1 segue a partir de uma lei lógica equivalente. Considere, por exemplo, a demonstração da Lei de DeMorgan 10(a):

$$(A \cup B)^C \quad \{x \mid x \notin (A \text{ ou } B)\} \quad \{x \mid x \notin A \text{ e } x \notin B\} \quad A^C \cap B^C$$

Aqui usamos a lei lógica equivalente (DeMorgan):

$$\neg(p \vee q) = \neg p \wedge \neg q$$

onde $\neg$ significa "não", $\vee$ significa "ou" e $\wedge$ significa "e". (Às vezes diagramas de Venn são empregados para ilustrar as leis na Tabela 1-1, como no Problema 1.17.)

Dualidade

As identidades na Tabela 1-1 são arranjadas em pares como, por exemplo, (2a) e (2b). Consideramos agora o princípio por trás desse arranjo. Suponha que E é uma equação de álgebra conjuntista. O dual E^* de E é a equação obtida pela substituição de cada ocorrência de $\cup$, $\cap$, $\mathbf{U}$ e $\emptyset$ em E por $\cap$, $\cup$, $\emptyset$ e $\mathbf{U}$, respectivamente. Por exemplo, o dual de

$$(\mathbf{U} \cap A) \cup (B \cap A) = A \quad \text{é} \quad (\emptyset \cup A) \cap (B \cup A) = A$$

Observe que os pares de leis na Tabela 1-1 são duais um do outro. É um fato da álgebra conjuntista, conhecido como *princípio de dualidade*, que se uma equação E é uma identidade, então seu dual E^* também é uma identidade.

1.6 CONJUNTOS FINITOS, PRINCÍPIO DA CONTAGEM

Conjuntos podem ser finitos ou infinitos. Um conjunto S é dito *finito* se S é vazio ou se S contém exatamente m elementos, onde m é um inteiro positivo; caso contrário, S é *infinito*.

Exemplo 1.7

(a) O conjunto A das letras do alfabeto inglês e o conjunto D dos dias da semana são finitos. Especificamente, A tem 26 elementos e D tem 7 elementos.

(b) Seja E o conjunto de inteiros positivos pares, e seja $\mathbf{I}$ o *intervalo unitário*, isto é,

$$E = \{2, 4, 6, \ldots\} \quad \text{e} \quad \mathbf{I} = [0, 1] = \{x \mid 0 \leq x \leq 1\}$$

Então E e $\mathbf{I}$ são infinitos.

Um conjunto S é *contável* se S é finito ou se os elementos de S podem ser arranjados como uma sequência. Neste último caso se diz que S é *infinito e contável*. Caso contrário, S é dito *não contável*. O conjunto E acima é infinito e contável, enquanto é possível demonstrar que o intervalo unitário $\mathbf{I} = [0, 1]$ é não contável.

Contando elementos em conjuntos finitos

A notação $n(S)$ ou $|S|$ denota o número de elementos em um conjunto S. (Alguns textos usam $\#(S)$ ou card(S) em vez de $n(S)$.) Assim, $n(A) = 26$, onde A é o conjunto das letras do alfabeto inglês, e $n(D) = 7$, onde D é o conjunto dos dias da semana. Além disso, $n(\emptyset) = 0$, uma vez que o conjunto vazio não tem elementos.

O lema a seguir se aplica.

Lema 1.6: Suponha que A e B são conjuntos finitos disjuntos. Então $A \cup B$ é finito e

$$n(A \cup B) = n(A) + n(B)$$

Esse lema pode ser reescrito como se segue:

Lema 1.6: Suponha que S é a união disjunta de conjuntos finitos A e B. Então S é finito e

$$n(S) = n(A) + n(B)$$

Prova. Ao contar os elementos de $A \cup B$, primeiro conte aqueles que estão em A. Há $n(A)$. Os únicos elementos restantes de $A \cup B$ são os que estão em B, mas não em A. Mas como B e A são disjuntos, nenhum elemento de B está em A e, portanto, há $n(B)$ elementos que estão em B, mas não em A. Logo, $n(A \cup B) = n(A) + n(B)$.

Para conjuntos quaisquer A e B, o conjunto A é a união disjunta de $A\backslash B$ e $A \cap B$. Assim, o Lema 1.6 nos garante o seguinte resultado útil.

Corolário 1.7: Sejam A e B conjuntos finitos. Então

$$n(A\backslash B) = n(A) - n(A \cap B)$$

Por exemplo, suponha que uma turma de artes A tenha 25 estudantes e 10 deles participam de uma turma de biologia B. Então o número de alunos na turma A que não está na turma B é:

$$n(A\backslash B) = n(A) - n(A \cap B) = 25 - 10 = 15$$

Dado qualquer conjunto A, lembre que o conjunto universo U é a união disjunta de A e A^C. Consequentemente, o Lema 1.6 também garante o seguinte resultado.

Corolário 1.8: Seja A um conjunto de um conjunto universo U. Então

$$n(A^C) = n(\mathrm{U}) - n(A)$$

Por exemplo, suponha que uma classe U com 30 estudantes tem 18 estudantes em tempo integral. Logo, há 30 - 18 = 12 estudantes em tempo parcial na classe U.

Princípio de inclusão-exclusão

Há uma fórmula para $n(A \cup B)$, mesmo quando eles não são disjuntos, chamada de Princípio de Inclusão-Exclusão, a saber:

Teorema (Princípio de Inclusão-Exclusão) 1.9: Suponha que A e B são conjuntos finitos. Então $A \cup B$ e $A \cap B$ são finitos e

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Ou seja, encontramos o número de elementos em A e B (ou ambos) somando $n(A)$ e $n(B)$ (inclusão) e então subtraindo $n(A \cap B)$ (exclusão), uma vez que seus elementos foram contados duas vezes.

Podemos aplicar esse resultado para obter uma fórmula semelhante para três conjuntos.

Corolário 1.10: Suponha que A, B e C sejam conjuntos finitos. Então $A \cup B \cup C$ é finito e

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Indução matemática (Seção 1.8) pode ser usada para generalizar esse resultado para qualquer número de conjuntos finitos.

Exemplo 1.8 Suponha que uma lista A contém os 30 estudantes de uma turma de matemática e que uma lista B contém os 35 estudantes de uma turma de inglês, e assuma que há 20 nomes em ambas as listas. Encontre o número de estudantes: (a) apenas na lista A, (b) apenas na lista B, (c) na lista A ou B (ou ambas), (d) em exatamente uma lista.

(a) A lista A tem 30 nomes e 20 estão na lista B, logo, $30 - 20 = 10$ nomes estão apenas na lista A.

(b) Analogamente, $35 - 20 = 15$ estão somente na lista B.

(c) Buscamos $n(A \cup B)$. Pela inclusão-exclusão,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B) = 30 + 35 - 20 = 45.$$

Em outras palavras, combinamos as duas listas e então eliminamos os 20 nomes que aparecem duas vezes.

(d) Por (a) e (b), $10 + 15 = 25$ nomes estão apenas em uma lista; isto é, $n(A \oplus B) = 25$

1.7 CLASSES DE CONJUNTOS, POTÊNCIAS, PARTIÇÕES

Dado um conjunto S, podemos querer falar sobre alguns de seus subconjuntos. Assim, consideraríamos um *conjunto de conjuntos*. Sempre que uma situação como essa ocorre, para evitar confusão, falaremos de uma *classe* de conjuntos ou *coleção* de conjuntos, em vez de um *conjunto* de conjuntos. Se desejarmos considerar alguns dos conjuntos de uma dada classe de conjuntos, então falamos de *subclasse* ou *subcoleção*.

Exemplo 1.9 Suponha $S = \{1, 2, 3, 4\}$.

(a) Seja A a classe de subconjuntos de S que contêm exatamente três elementos de S. Então

$$A = [\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}]$$

Isto é, os elementos de A são os conjuntos $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$ e $\{2, 3, 4\}$.

(b) Seja B a classe de subconjuntos de S, sendo que cada um contém o 2 e dois outros elementos de S. Então

$$B = [\{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}]$$

Os elementos de B são os conjuntos $\{1, 2, 3\}$, $\{1, 2, 4\}$ e $\{2, 3, 4\}$. Logo, B é uma subclasse de A, uma vez que todo elemento de B é também um elemento de A. (Para evitar confusão, às vezes envolvemos os conjuntos de uma classe entre colchetes em vez de entre chaves.)

Potência

Para um dado conjunto S, podemos falar da classe de todos os subconjuntos de S. Essa classe é chamada de *potência* de S, e é denotada por $P(S)$. Se S é finito, então $P(S)$ também o é. De fato, o número de elementos em $P(S)$ é 2 elevado à potência $n(S)$. Ou seja,

$$n(P(S)) = 2^{n(S)}$$

(Por esse motivo, o conjunto potência de S é às vezes denotado por 2^S.)

Exemplo 1.10 Suponha que $S = \{1, 2, 3\}$. Logo,

$$P(S) = [\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, S]$$

Note que o conjunto vazio $\emptyset$ pertence a $P(S)$, uma vez que $\emptyset$ é um subconjunto de S. Analogamente, S pertence a $P(S)$. Como esperado da observação acima, $P(S)$ tem $2^3 = 8$ elementos.

Partições

Seja S um conjunto não vazio. Uma *partição* de S é uma subdivisão de S em conjuntos disjuntos e não vazios. Precisamente, uma *partição* de S é uma coleção $\{A_i\}$ de subconjuntos não vazios de S tal que:

(i) Cada a em S pertence a um dos A_i.

(ii) Os conjuntos de $\{A_i\}$ são mutuamente disjuntos, isto é, se

$$A_j \neq A_k \quad \text{então} \quad A_j \cap A_k = \emptyset$$

Os subconjuntos em uma partição são chamados de *células*. A Fig. 1-6 é um diagrama de Venn de uma partição do conjunto retangular S de pontos em cinco células, A_1, A_2, A_3, A_4 e A_5.

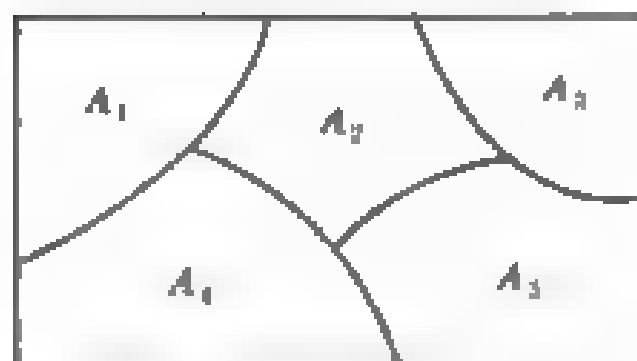



Figura 1-6

Exemplo 1.11 Considere as seguintes coleções de subconjuntos de $S = \{1, 2, \ldots, 8, 9\}$.

(i) $[\{1, 3, 5\}, \{2, 6\}, \{4, 8, 9\}]$
(ii) $[\{1, 3, 5\}, \{2, 4, 6, 8\}, \{5, 7, 9\}]$
(iii) $[\{1, 3, 5\}, \{2, 4, 6, 8\}, \{7, 9\}]$

Então (i) não é uma partição de S, uma vez que 7 em S não pertence a qualquer um dos subconjuntos. Além disso, (ii) não é uma partição de S, pois $\{1, 3, 5\}$ e $\{5, 7, 9\}$ não são disjuntos. Por outro lado, (iii) é uma partição de S

Operações conjuntistas generalizadas

As operações conjuntistas de união e interseção foram definidas acima para dois conjuntos. Essas operações podem ser estendidas para qualquer quantia de conjuntos, finita ou infinita, como se segue.

Considere primeiro um número finito de conjuntos, digamos, $A_1, A_2, \ldots, A_m$. A união e a interseção desses conjuntos são denotadas, respectivamente, por

$$A_1 \cup A_2 \cup \ldots \cup A_m = \bigcup_{i=1}^{m} A_i = \{x \mid x \in A_i \text{ para algum } A_i\}$$
$$A_1 \cap A_2 \cap \ldots \cap A_m = \bigcap_{i=1}^{m} A_i = \{x \mid x \in A_i \text{ para todo } A_i\}$$

Ou seja, a união consiste naqueles elementos que pertencem a pelo menos um dos conjuntos, e a interseção consiste nos elementos que pertencem a todos os conjuntos.

Agora, seja $\mathscr{A}$ uma coleção qualquer de conjuntos. A união e a interseção dos conjuntos na coleção $\mathscr{A}$ são denotadas e definidas, respectivamente, por

$$\bigcup(A \mid A \in \mathscr{A}) = \{x \mid x \in A_i \text{ para algum } A_i \in \mathscr{A}\}$$
$$\bigcap(A \mid A \in \mathscr{A}) = \{x \mid x \in A_i \text{ para todo } A_i \in \mathscr{A}\}$$

Ou seja, a união consiste naqueles elementos que pertencem a pelo menos um dos conjuntos na coleção $\mathscr{A}$, e a interseção consiste nos elementos que pertencem a cada conjunto na coleção A.

Exemplo 1.12 Considere os conjuntos

$$A_1 = \{1, 2, 3, \ldots\} = \mathbf{N}, \quad A_2 = \{2, 3, 4, \ldots\}, \quad A_3 = \{3, 4, 5, \ldots\}, \quad A_n = \{n, n+1, n+2, \ldots\}.$$

Então a união e a interseção dos conjuntos são como se segue:

$$\bigcup(A_k \mid k \in \mathbf{N}) = \mathbf{N} \quad \text{e} \quad \bigcap(A_k \mid k \in \mathbf{N}) = \emptyset$$

As Leis de DeMorgan valem também para as operações generalizadas acima. Isto é:

Teorema 1.11: Seja $\mathscr{A}$ uma coleção de conjuntos. Então:

(i) $\left[\bigcup(A \mid A \in \mathscr{A})\right]^C = \bigcap(A^C \mid A \in \mathscr{A})$
(ii) $\left[\bigcap(A \mid A \in \mathscr{A})\right]^C = \bigcup(A^C \mid A \in \mathscr{A})$

1.8 INDUÇÃO MATEMÁTICA

Uma propriedade essencial do conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ de inteiros positivos segue abaixo:

Princípio de Indução Matemática I: Seja P uma proposição definida sobre os inteiros positivos $\mathbf{N}$; isto é, $P(n)$ é verdadeira ou falsa para cada $n \in \mathbf{N}$. Suponha que P tem as duas propriedades a seguir:

(i) $P(1)$ é verdadeira.

(ii) $P(k + 1)$ é verdadeira sempre que $P(k)$ for verdadeira.

Então P é verdadeira para todo inteiro positivo $n \in \mathbf{N}$.

Não demonstraremos esse princípio. De fato, ele geralmente é dado como um dos axiomas quando $\mathbf{N}$ é desenvolvido axiomaticamente.

Exemplo 1.13 Seja P a proposição de que a soma dos primeiros n números ímpares é n^2; ou seja,

$$P(n): 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

(O k-ésimo número ímpar é $2k - 1$, e o próximo número ímpar é $2k + 1$.) Observe que $P(n)$ é verdadeira para $n = 1$, a saber,

$$P(1): 1 = 1^2$$

Assumindo que $P(k)$ é verdadeira, adicionamos $2k + 1$ a ambos os lados, obtendo

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2$$

o que é $P(k + 1)$. Em outras palavras, $P(k + 1)$ é verdadeira quando $P(k)$ é verdadeira. Pelo Princípio de Indução Matemática, P é verdadeira para todo n.

Existe uma forma do Princípio da Indução Matemática que é, às vezes, mais conveniente para usar. Apesar de parecer diferente, é realmente equivalente ao princípio de indução acima.

Princípio de Indução Matemática II: Seja P uma proposição definida sobre os inteiros positivos $\mathbf{N}$, tal que:

(i) $P(1)$ é verdadeira.

(ii) $P(k)$ é verdadeira quando $P(j)$ é verdadeira para todo $1 \leq j < k$.

Então P é verdadeira para todo inteiro positivo $n \in \mathbf{N}$.

Observação: Eventualmente pode se querer provar que uma proposição P é verdadeira para o conjunto de inteiros

$$\{a, a + 1, a + 2, a + 3, \ldots\}$$

onde a é qualquer inteiro, podendo ser zero. Isso pode ser feito simplesmente substituindo 1 por a em qualquer um dos Princípios de Indução Matemática.

Problemas Resolvidos

Conjuntos e subconjuntos

1.1 Quais destes conjuntos são iguais: $\{x, y, z\}$, $\{z, y, z, x\}$, $\{y, x, y, z\}$, $\{y, z, x, y\}$?

Eles são todos iguais. Ordem e repetição não mudam um conjunto.

1.2 Liste os elementos de cada conjunto, onde $\mathbf{N} = \{1, 2, 3, \ldots\}$.

(a) $A = \{x \in \mathbf{N} \mid 3 < x < 9\}$

(b) $B = \{x \in \mathbf{N} \mid x \text{ é par}, x < 11\}$

(c) $C = \{x \in \mathbf{N} \mid 4 + x = 3\}$

(a) A consiste nos inteiros positivos entre 3 e 9; logo, $A = \{4, 5, 6, 7, 8\}$.

(b) B consiste nos inteiros positivos pares menores do que 11; logo, $B = \{2, 4, 6, 8, 10\}$.

(c) Nenhum inteiro positivo satisfaz $4 + x = 3$; logo, $C = \emptyset$, o conjunto vazio.

1.3 Seja $A = \{2, 3, 4, 5\}$.

(a) Mostre que A não é um subconjunto de $B = \{x \in \mathbf{N} \mid x \text{ é par}\}$

(b) Mostre que A é um subconjunto próprio de $C = \{1, 2, 3, \ldots, 8, 9\}$.

(a) É necessário mostrar que pelo menos um elemento em A não pertence a B. Agora, $3 \in A$ e, como B consiste em números pares, $3 \notin B$, logo, A não é subconjunto de B.

(b) Cada elemento de A pertence a C, portanto $A \subseteq C$. Por outro lado, $1 \in C$, mas $1 \notin A$. Logo, $A \neq C$. Assim, A é um subconjunto próprio de C.

Operações conjuntistas

1.4 Seja $\mathbf{U} = \{1, 2, \ldots, 9\}$ o conjunto universo, e sejam

$$A = \{1, 2, 3, 4, 5\}, \quad C = \{5, 6, 7, 8, 9\}, \quad E = \{2, 4, 6, 8\},$$
$$B = \{4, 5, 6, 7\}, \quad D = \{1, 3, 5, 7, 9\}, \quad F = \{1, 5, 9\}.$$

Encontre: (a) $A \cup B$ e $A \cap B$; (b) $A \cup C$ e $A \cap C$; (c) $D \cup F$ e $D \cap F$.

Lembre que a união $X \cup Y$ consiste naqueles elementos em X ou Y (ou ambos), e a interseção $X \cap Y$ consiste nos elementos em ambos X e Y.

(a) $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$ e $A \cap B = \{4, 5\}$

(b) $A \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} = \mathbf{U}$ e $A \cap C = \{5\}$

(c) $D \cup F = \{1, 3, 5, 7, 9\} = D$ e $D \cap F = \{1, 5, 9\} = F$

Observe que $F \subseteq D$. Portanto, pelo Teorema 1.4, devemos ter $D \cup F = D$ e $D \cap F = F$.

1.5 Considere os conjuntos no Problema 1.4. Encontre:

(a) A^C, B^C, D^C, E^C; (b) $A \backslash B, B \backslash A, D \backslash E, F \backslash D$; (c) $A \oplus B, C \oplus D, E \oplus F$.

Lembre que:

(1) Os complementares X^C consistem naqueles elementos em $\mathbf{U}$ que não pertencem a X.

(2) A diferença $X \backslash Y$ consiste nos elementos em X que não pertencem a Y.

(3) A diferença simétrica $X \oplus Y$ consiste nos elementos em X ou Y, mas não em ambos.

Portanto:

(a) $A^C = \{6, 7, 8, 9\}$, $B^C = \{1, 2, 3, 8, 9\}$, $D^C = \{2, 4, 6, 8\} = E$, $E^C = \{1, 3, 5, 7, 9\} = D$

(b) $A \backslash B = \{1, 2, 3\}$; $B \backslash A = \{6, 7\}$; $D \backslash E = \{1, 3, 5, 7, 9\} = D$; $F \backslash D = \emptyset$.

(c) $A \oplus B = \{1, 2, 3, 6, 7\}$, $C \oplus D = \{1, 3, 6, 8\}$, $E \oplus F = \{2, 4, 6, 8, 1, 5, 9\} = E \cup F$.

1.6 Mostre que podemos ter: (a) $A \cap B = A \cap C$ sem $B = C$; (b) $A \cup B = A \cup C$ sem $B = C$

(a) Sejam $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{2, 4\}$. Então, $A \cap B = \{2\}$ e $A \cap C = \{2\}$, mas $B \neq C$.

(b) Sejam $A = \{1, 2\}$, $B = \{1, 3\}$, $C = \{2, 3\}$. Então, $A \cup B = \{1, 2, 3\}$ e $A \cup C = \{1, 2, 3\}$, mas $B \neq C$.

1.7 Demonstre: $B \backslash A = B \cap A^C$. Assim, a operação conjuntista de diferença pode ser escrita em termos das operações de interseção e complementar.

$$B \backslash A = \{x \mid x \in B, x \notin A\} = \{x \mid x \in B, x \in A^C\} = B \cap A^C.$$

1.8 Prove o Teorema 1.4. As fórmulas a seguir são equivalentes: $A \subset B$, $A \cap B = A$, $A \cup B = B$

Suponha que $A \subseteq B$ e faça $x \in A$. Então $x \in B$ e, portanto, $x \in A \cap B$ e $A \subset A \cap B$. Pelo Teorema 1.3, $(A \cap B) \subset A$. Assim, $A \cap B = A$. Por outro lado, suponha que $A \cap B = A$ e faça $x \in A$. Então, $x \in (A \cap B)$; logo, $x \in A$ e $x \in B$. Portanto, $A \subseteq$ B. Ambos os resultados mostram que $A \subseteq B$ é equivalente a $A \cap B = A$.

Suponha novamente que $A \subset B$. Faça $x \in (A \cup B)$. Então, $x \in A$ ou $x \in B$. Se $x \in A$, então $x \in B$, pois $A \subset B$. Em qualquer caso, $x \in B$. Portanto, $A \cup B \subseteq B$. Pelo Teorema 1.3, $B \subseteq A \cup B$. Assim, $A \cup B = B$. Agora suponha que $A \cup B = B$ e faça $x \in A$. Então, $x \in A \cup B$, pela definição de união de conjuntos. Logo, $x \in B = A \cup B$. Portanto, $A \subseteq B$. Ambos os resultados mostram que $A \subset B$ é equivalente a $A \cup B = B$.

Assim, $A \subseteq B$, $A \cup B = A$ e $A \cup B = B$ são equivalentes.

Diagramas de Venn, álgebra de conjuntos, dualidade

1.9 Ilustre a Lei de DeMorgan $(A \cup B)^C = A^C \cap B^C$ usando diagramas de Venn.

Sombreie a área fora de $A \cup B$ em um diagrama de Venn de conjuntos A e B. Isso é mostrado na Fig. 1-7(*a*), logo, a área sombreada representa $(A \cup B)^C$. Agora sombreie a área fora de A em um diagrama de Venn de A e B com barras em uma direção (//, /), e então sombreie a área fora de B com barras em outra direção (\\, \\). Isso é mostrado na Fig. 1-7(*b*), logo, a área com barras cruzadas (a área com ambas as barras presentes) representa $A^C \cap B^C$. Ambos $(A \cup B)^C$ e $A^C \cap B^C$ são representados pela mesma área, assim, o diagrama de Venn indica que $(A \cup B)^C = A^C \cap B^C$. (Enfatizamos que um diagrama de Venn não é uma demonstração formal, mas pode indicar relações entre conjuntos.)

(*a*)

(*b*)

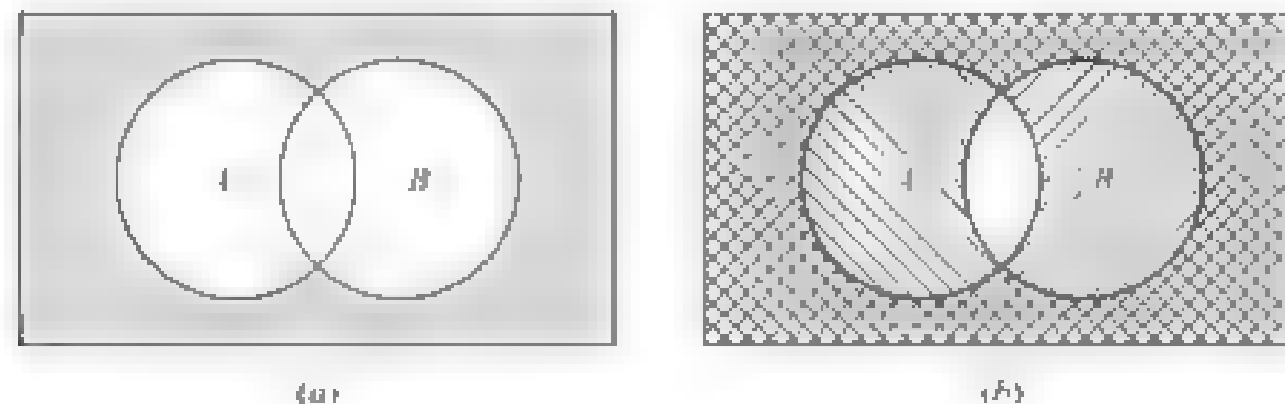



Figura 1-7

1.10 Demonstre a Lei Distributiva: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$$A \cap (B \cup C) = \{x \mid x \in A, x \in (B \cup C)\}$$
$$= \{x \mid x \in A, x \in B \text{ ou } x \in A, x \in C\} = (A \cap B) \cup (A \cap C)$$

Aqui empregamos a lei lógica análoga $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$, onde $\wedge$ denota "e" e $\vee$ denota "ou".

1.11 Escreva o dual de: (a) $(U \cap A) \cup (B \cap A) = A$, (b) $(A \cap U) \cap (\emptyset \cup A^C) = \emptyset$

Permute $\cup$ com $\cap$ e também U com $\emptyset$ em cada equação conjuntista.

(a) $(\emptyset \cup A) \cap (B \cup A) = A$, (b) $(A \cup \emptyset) \cup (U \cap A^C) = U$

1.12 Prove: $(A \cup B)\backslash(A \cap B) = (A\backslash B) \cup (B\backslash A)$. (Assim, qualquer um dos dois pode ser usado para definir $A \oplus B$.)

Usando $X\backslash Y = X \cap Y^C$ e as leis da Tabela 1.1, incluindo a Lei de DeMorgan, obtemos:

$$\begin{aligned}(A \cup B)\backslash(A \cap B) &= (A \cup B) \cap (A \cap B)^C = (A \cup B) \cap (A^C \cup B^C)\\ &= (A \cup A^C) \cup (A \cap B^C) \cup (B \cap A^C) \cup (B \cap B^C)\\ &= \emptyset \cup (A \cap B^C) \cup (B \cap A^C) \cup \emptyset\\ &= (A \cap B^C) \cup (B \cap A^C) = (A\backslash B) \cup (B\backslash A)\end{aligned}$$

1.13 Determine a validade do seguinte argumento:

S_1: Todos os meus amigos são músicos.
S_2: João é meu amigo.
S_3: Nenhum dos meus vizinhos é músico.

S: João não é meu vizinho.

As premissas S_1 e S_3 conduzem ao diagrama de Venn na Fig. 1-8(*a*). De acordo com S_2, João pertence ao conjunto de amigos que é disjunto do conjunto de vizinhos. Assim, S é uma conclusão válida e, portanto, o argumento é válido.

(*a*)

(*b*)

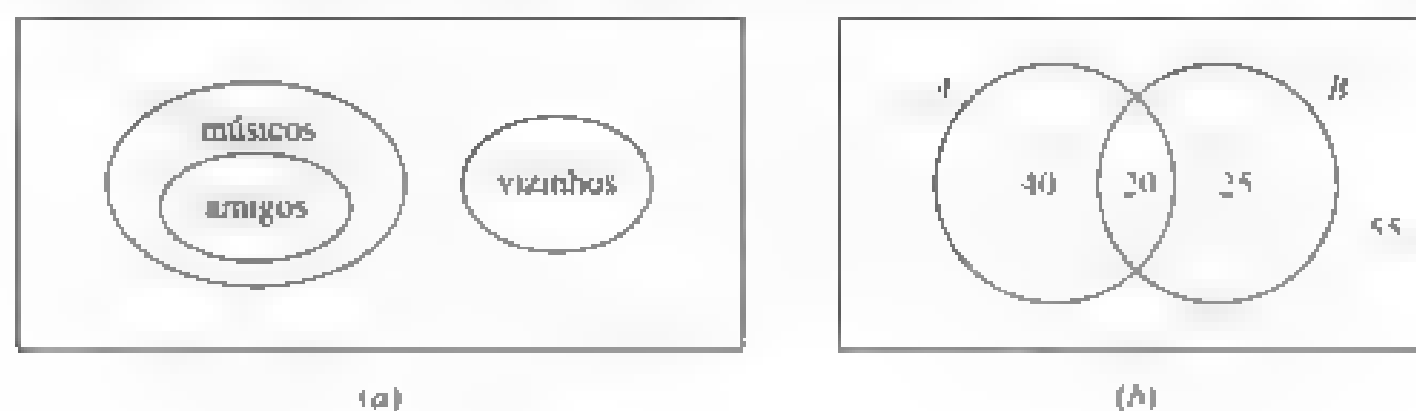



Figura 1-8

Conjuntos finitos e o princípio da contagem

1.14 Cada estudante de Artes Liberais em alguma faculdade tem um requisito A em matemática e um requisito B em ciências. Uma pesquisa com 140 estudantes veteranos mostra que:

60 completaram A, 45 completaram B, 20 completaram A e B

Use um diagrama de Venn para encontrar o número de estudantes que completaram:

(a) Pelo menos um entre A e B; (b) exatamente um entre A ou B, (c) nem A, nem B.

Traduzindo os dados acima em notação conjuntista temos:

$$n(A) = 60, n(B) = 45, n(A \cap B) = 20, n(\mathbf{U}) = 140$$

Esboce um diagrama de Venn dos conjuntos A e B, como na Fig. 1-1(*c*). Em seguida, como na Fig. 1-8(*b*), assinale números às quatro regiões como se segue:

20 completaram ambos A e B; assim, $n(A \cap B) = 20$.

$60 - 20 = 40$ completaram A, mas não B; portanto, $n(A \backslash B) = 40$.

$45 - 20 = 25$ completaram B, mas não A, assim, $n(B \backslash A) = 25$.

$140 - 20 - 40 - 25 = 55$ não completaram requisito algum.

Pelo diagrama de Venn.

(a) $20 + 40 + 25 = 85$ completaram A ou B. Alternadamente, pelo Princípio de Inclusão-Exclusão,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B) = 60 + 45 - 20 = 85$$

(b) $40 + 25 = 65$ completaram exatamente um requisito. Ou seja, $n(A \oplus B) = 65$.

(c) 55 não completaram requisito algum, isto é, $n(A^C \cap B^C) = n[(A \cup B)^C] = 140 - 85 = 55$.

1.15 Em uma pesquisa com 120 pessoas, foi descoberto que:

65 leem a revista *Newsweek*, 20 leem *Newsweek* e *Time*,
45 leem *Time*, 25 leem *Newsweek* e *Fortune*,
42 leem *Fortune*, 15 leem *Time* e *Fortune*,
8 leem as três revistas.

(a) Encontre o número de pessoas que leem pelo menos uma das três revistas.

(b) Preencha o número correto de pessoas em cada uma das oito regiões do diagrama de Venn na Fig. 1-9(*a*), onde N, T e F denotam os conjuntos de pessoas que leem *Newsweek*, *Time* e *Fortune*, respectivamente.

(c) Encontre o número de pessoas que leem somente uma revista.

(*a*) (*b*)

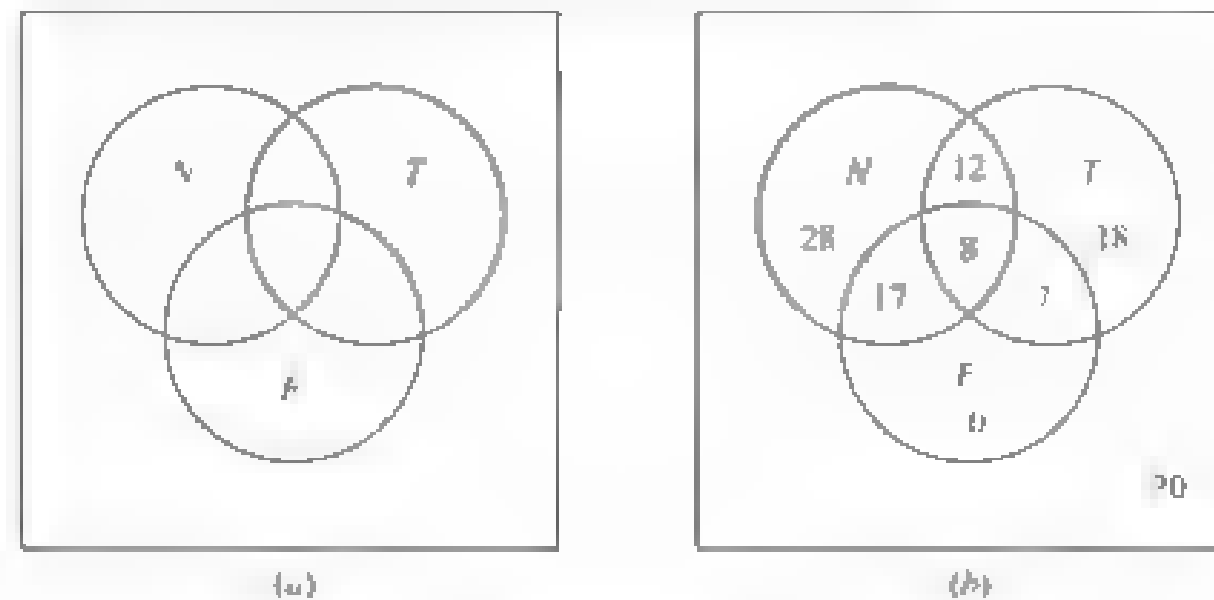



Figura 1-9

(a) Queremos encontrar $n(N \cup T \cup F)$. Pelo Corolário 1.10 (Princípio de Inclusão-Exclusão),

$$n(N \cup T \cup F) = n(N) + n(T) + n(F) - n(N \cap T) - n(N \cap F) - n(T \cap F) + n(N \cap T \cap F)$$
$$= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100$$

(b) O diagrama de Venn pedido na Fig. 1-9 (*b*) é obtido como se segue:

8 leem as três revistas,

$20 - 8 = 12$ leem *Newsweek* e *Time*, mas não as três revistas,

$25 - 8 = 17$ leem *Newsweek* e *Fortune*, mas não as três revistas,

$15 - 8 = 7$ leem *Time* e *Fortune*, mas não as três revistas,

$65 - 12 - 8 - 17 = 28$ leem apenas *Newsweek*,

$45 - 12 - 8 - 7 = 18$ leem apenas *Time*,

$42 - 17 - 8 - 7 = 10$ leem apenas *Fortune*,

$120 - 100 = 20$ não leem revista alguma.

(c) $28 + 18 + 10 = 56$ leem somente uma das revistas.

1.16 Prove o Teorema 1.9. Suponha que A e B são conjuntos finitos. Então, $A \cup B$ e $A \cap B$ são finitos e

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Se A e B são conjuntos finitos, claramente $A \cup B$ e $A \cap B$ são finitos.

Suponha que contemos os elementos em A e então os elementos em B.

Logo, todo elemento em $A \cap B$ seria contado duas vezes, uma vez em A e outra em B. Portanto,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Classes de conjuntos

1.17 Seja $A = [\{1, 2, 3\}, \{4, 5\}, \{6, 7, 8\}]$. (a) Liste os elementos de A. (b) Encontre $n(A)$.

(a) A tem três elementos, os conjuntos $\{1, 2, 3\}$, $\{4, 5\}$ e $\{6, 7, 8\}$.

(b) $n(A) = 3$.

1.18 Determine a potência $P(A)$ de $A = \{a, b, c, d\}$.

Os elementos de $P(A)$ são os subconjuntos de A. Logo,

$$P(A) = [A, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a\}, \{b\}, \{c\}, \{d\}, \emptyset]$$

Como esperado, $P(A)$ tem $2^4 = 16$ elementos.

1.19 Seja $S = \{a, b, c, d, e, f, g\}$. Determine quais dos conjuntos a seguir são partições de S:

(a) $P_1 = [\{a, c, e\}, \{b\}, \{d, g\}]$, (c) $P_3 = [\{a, b, e, g\}, \{c\}, \{d, f\}]$,
(b) $P_2 = [\{a, e, g\}, \{c, d\}, \{b, e, f\}]$, (d) $P_4 = [\{a, b, c, d, e, f, g\}]$.

(a) P_1 não é uma partição de S, uma vez que $f \in S$ não pertence a qualquer uma das células.

(b) P_2 não é uma partição de S, uma vez que $e \in S$ pertence a duas das células.

(c) P_3 é uma partição de S, uma vez que cada elemento de S pertence a exatamente uma célula.

(d) P_4 é uma partição de S em uma célula, o próprio S.

1.20 Encontre todas as partições de $S = \{a, b, c, d\}$.

Observe primeiramente que cada partição de S contém uma, duas, três ou quatro células distintas. As partições são como se segue:

(1) $[\{a, b, c, d\}]$

(2) $[\{a\}, \{b, c, d\}], [\{b\}, \{a, c, d\}], [\{c\}, \{a, b, d\}], [\{d\}, \{a, b, c\}],$
$[\{a, b\}, \{c, d\}], [\{a, c\}, \{b, d\}], [\{a, d\}, \{b, c\}]$

(3) $[\{a\}, \{b\}, \{c, d\}], [\{a\}, \{c\}, \{b, d\}], [\{a\}, \{d\}, \{b, c\}],$
$[\{b\}, \{c\}, \{a, d\}], [\{b\}, \{d\}, \{a, c\}], [\{c\}, \{d\}, \{a, b\}]$

(4) $[\{a\}, \{b\}, \{c\}, \{d\}]$

Há 15 partições diferentes de S.

1.21 Seja $\mathbf{N} = \{1, 2, 3, \ldots\}$ e, para cada $n \in \mathbf{N}$, faça $A_n = \{n, 2n, 3n, \ldots\}$. Encontre:

(a) $A_3 \cap A_5$; (b) $A_4 \cap A_5$; (c) $\bigcup_{i \in Q} A_i$, onde $Q = \{2, 3, 5, 7, 11, \ldots\}$ é o conjunto de números primos.

(a) Aqueles números que são múltiplos de 3 e 5 são múltiplos de 15; logo, $A_3 \cap A_5 = A_{15}$.

(b) Os múltiplos de 12 e de nenhum outro número pertencem a ambos A_4 e A_6, logo, $A_4 \cap A_6 = A_{12}$

(c) Todo inteiro positivo, exceto 1, é um múltiplo de pelo menos um número primo; logo,

$$\bigcup_{i \in Q} A_i = \{2, 3, 4, \ldots\} = \mathbf{N} \backslash \{1\}$$

1.22 Seja $\{A_i \mid i \in I\}$ uma classe indexada de conjuntos e considere $i_0 \in I$. Prove que

$$\bigcap_{i \in I} A_i \subset A_{i_0} \subset \bigcup_{i \in I} A_i$$

Seja $x \in \bigcap_{i \in I} A_i$. Então $x \in A_i$ para todo $i \in I$. Em particular, $x \in A_{i_0}$. Logo, $\bigcap_{i \in I} A_i \subseteq A_{i_0}$. Agora considere $y \in A_{i_0}$. Como $i_0 \in I$, $y \in \bigcap_{i \in I} A_i$. Portanto, $A_{i_0} \subseteq \bigcap_{i \in I} A_i$.

1.23 Prove (Lei de DeMorgan): Para qualquer classe indexada $\{A_i \mid i \in I\}$, temos $(\bigcup_i A_i)^C = \bigcap_i A_i^C$

Usando a definição de união e interseção de classes indexadas de conjuntos:

$$(\bigcup_i A_i)^C = \{x \mid x \notin \bigcup_i A_i\} = \{x \mid x \notin A_i \text{ para todo } i\}$$
$$= \{x \mid x \in A_i^C \text{ para todo } i\} = \bigcap_i A_i^C$$

Indução matemática

1.24 Demonstre a proposição $P(n)$ que afirma que a soma dos primeiros n inteiros positivos é $\frac{1}{2}n(n+1)$; ou seja,

$$P(n) = 1 + 2 + 3 + \cdots + n = \tfrac{1}{2}n(n+1)$$

A proposição vale para $n = 1$, uma vez que:

$$P(1): 1 = \tfrac{1}{2}(1)(1+1)$$

Assumindo que $P(k)$ é verdadeira, somamos $k + 1$ em ambos os lados de $P(k)$, obtendo

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k+1) &= \tfrac{1}{2}k(k+1) + (k+1) \\ &= \tfrac{1}{2}[k(k+1) + 2(k+1)] \\ &= \tfrac{1}{2}[(k+1)(k+2)] \end{aligned}$$

que resulta em $P(k+1)$. Isto é, $P(k+1)$ é verdadeira quando $P(k)$ é verdadeira. Pelo Princípio de Indução, P é verdadeira para todo n.

1.25 Prove a seguinte proposição (para $n \geq 0$):

$$P(n): 1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$$

$P(0)$ é verdadeira, uma vez que $1 = 2^1 - 1$. Assumindo que $P(k)$ é verdadeira, somamos 2^{k+1} a ambos os lados de $P(k)$, obtendo

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1} = 2(2^{k+1}) - 1 = 2^{k+2} - 1$$

que resulta em $P(k+1)$. Isto é, $P(k+1)$ é verdadeira se $P(k)$ é verdadeira. Pelo Princípio de Indução, $P(n)$ é verdadeira para todo n.

Problemas Complementares

Conjuntos e subconjuntos

1.26 Quais dos conjuntos a seguir são iguais?

$A = \{x \mid x^2 - 4x + 3 = 0\}$, $C = \{x \mid x \in \mathbf{N}, x < 3\}$, $E = \{1, 2\}$, $G = \{3, 1\}$,
$B = \{x \mid x^2 - 3x + 2 = 0\}$, $D = \{x \mid x \in \mathbf{N}, x$ é ímpar, $x < 5\}$, $F = \{1, 2, 1\}$, $H = \{1, 1, 3\}$.

1.27 Liste os elementos dos conjuntos a seguir se o conjunto universo é $\mathbf{U} = \{a, b, c, \ldots, y, z\}$.

Além disso, identifique quais dos conjuntos, se for o caso, são iguais.

$A = \{x \mid x$ é uma vogal$\}$ $C = \{x \mid x$ precede f no alfabeto$\}$,
$B = \{x \mid x$ é uma letra da palavra "little"$\}$, $D = \{x \mid x$ é uma letra da palavra "title"$\}$

1.28 Sejam $A = \{1, 2, \ldots, 8, 9\}$, $B = \{2, 4, 6, 8\}$, $C = \{1, 3, 5, 7, 9\}$, $D = \{3, 4, 5\}$ e $E = \{3, 5\}$

Quais desses conjuntos podem ser iguais a um conjunto X sob cada uma das condições seguintes?

(a) X e B são disjuntos. (c) $X \subseteq A$, mas $X \not\subset C$.
(b) $X \subset D$, mas $X \not\subset B$ (d) $X \subset C$, mas $X \not\subset A$.

Operações conjuntistas

1.29 Considere o conjunto universo $\mathbf{U} = \{1, 2, 3, \ldots, 8, 9\}$ e os conjuntos $A = \{1, 2, 5, 6\}$, $B = \{2, 5, 7\}$, $C = \{1, 3, 5, 7, 9\}$. Encontre:

(a) $A \cap B$ e $A \cap C$ (c) A^C e C^C (e) $A \oplus B$ e $A \oplus C$
(b) $A \cup B$ e $B \cup C$ (d) $A \backslash B$ e $A \backslash C$ (f) $(A \cup C) \backslash B$ e $(B \oplus C) \backslash A$

1.30 Sejam A e B conjuntos quaisquer. Prove.

(a) A é a união disjunta de $A \setminus B$ com $A \cap B$.

(b) $A \cup B$ é a união disjunta entre $A \setminus B$, $A \cap B$ e $B \setminus A$.

1.31 Prove o que se segue:

(a) $A \subseteq B$ se, e somente se, $A \cap B^C = \emptyset$ (c) $A \subseteq B$ se, e somente se, $B^C \subseteq A^C$

(b) $A \subseteq B$ se, e somente se, $A^C \cup B = \mathbf{U}$ (d) $A \subseteq B$ se, e somente se, $A \setminus B = \emptyset$

(Compare os resultados com o Teorema 1.4.)

1.32 Demonstre as Leis de Absorção: (a) $A \cup (A \cap B) = A$; (b) $A \cap (A \cup B) = A$.

1.33 A fórmula $A \setminus B = A \cap B^C$ define a operação de diferença em termos das operações de interseção e complementar. Encontre uma fórmula que defina a união $A \cup B$ em termos das operações de interseção e complementar.

Diagramas de Venn

1.34 O diagrama de Venn na Fig. 1-5(a) exibe conjuntos A, B e C. Sombreie os seguintes conjuntos.

(a) $A \setminus (B \cup C)$; (b) $A^C \cap (B \cup C)$; (c) $A^C \cap (C \setminus B)$.

1.35 Use o diagrama de Venn da Fig. 1-5(b) para escrever cada conjunto como a união (disjunta) de produtos fundamentais.

(a) $A \cap (B \cup C)$; (b) $A^C \cap (B \cup C)$; (c) $A \cup (B \setminus C)$.

1.36 Considere as seguintes premissas:

S_1: Todos os dicionários são úteis.

S_2: Maria possui apenas romances.

S_3: Nenhum romance é útil.

Use um diagrama de Venn para determinar a validade de cada uma das seguintes conclusões.

(a) Romances não são dicionários.

(b) Maria não possui um dicionário.

(c) Todos os livros úteis são dicionários.

Álgebra de conjuntos e dualidade

1.37 Escreva o dual de cada equação:

(a) $A = (B^C \cap A) \cup (A \cap B)$

(b) $(A \cap B) \cup (A^C \cap B) \cup (A \cap B^C) \cup (A^C \cap B^C) = \mathbf{U}$

1.38 Use as leis da Tabela 1-1 para provar cada identidade conjuntista:

(a) $(A \cap B) \cup (A \cap B^C) = A$

(b) $A \cup B = (A \cap B^C) \cup (A^C \cap B) \cup (A \cap B)$

Conjuntos finitos e o princípio da contagem

1.39 Determine quais dos seguintes conjuntos são finitos:

(a) Retas paralelas ao eixo x. (c) Inteiros que são múltiplos de 5.

(b) Letras do alfabeto inglês. (d) Animais vivendo sobre a Terra.

1.40 Use o Teorema 1.9 para provar o Corolário 1.10: Suponha que A, B e C são conjuntos finitos. Então $A \cup B \cup C$ é finito e

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

1.41 Um levantamento sobre uma amostra de 25 carros novos sendo vendidos em uma loja de automóveis foi conduzido para perceber quais das três opções populares, ar-condicionado (A), rádio (R) e vidro elétrico (V), já foram instaladas. O levantamento descobriu que:

15 tinham ar-condicionado (A),	5 tinham A e V,	
12 tinham rádio (R),	9 tinham A e R,	3 tinham todas as opções.
11 tinham vidro elétrico (V),	4 tinham R e V,	

Encontre o número de carros que tinham (a) apenas V; (b) apenas A, (c) apenas R, (d) R e V, mas não A, (e) A e R, mas não V; (f) apenas uma das opções; (g) pelo menos uma opção; (h) nenhuma das opções.

Classes de conjuntos

1.42 Encontre o conjunto potência $P(A)$ de $A = \{1, 2, 3, 4, 5\}$.

1.43 Dado $A = [\{a, b\}, \{c\}, \{d, e, f\}]$.

(a) liste os elementos de A, (b) encontre $n(A)$, (c) encontre a potência de A.

1.44 Suponha que A é finito e $n(A) = m$. Demonstre que o conjunto potência $P(A)$ tem 2^m elementos.

Partições

1.45 Seja $S = \{1, 2, \ldots, 8, 9\}$. Determine se cada um dos conjuntos a seguir é uma partição de S:

(a) $[\{1, 3, 6\}, \{2, 8\}, \{5, 7, 9\}]$ (c) $[\{2, 4, 5, 8\}, \{1, 9\}, \{3, 6, 7\}]$

(b) $[\{1, 5, 7\}, \{2, 4, 8, 9\}, \{3, 5, 6\}]$ (d) $[\{1, 2, 7\}, \{3, 5\}, \{4, 6, 8, 9\}, \{3, 5\}]$

1.46 Seja $S = \{1, 2, 3, 4, 5, 6\}$. Determine se cada um dos conjuntos a seguir é uma partição de S:

(a) $P_1 = [\{1, 2, 3\}, \{1, 4, 5, 6\}]$ (c) $P_3 = [\{1, 3, 5\}, \{2, 4\}, \{6\}]$

(b) $P_2 = [\{1, 2\}, \{3, 5, 6\}]$ (d) $P_4 = [\{1, 3, 5\}, \{2, 4, 6, 7\}]$

1.47 Determine se cada um dos conjuntos a seguir é uma partição do conjunto **N** dos inteiros positivos.

(a) $[\{n \mid n > 5\}, \{n \mid n < 5\}]$; (b) $[\{n \mid n > 6\}, \{1, 3, 5\}, \{2, 4\}]$;

(c) $[\{n \mid n^2 > 11\}, \{n \mid n^2 < 11\}]$

1.48 Sejam $[A_1, A_2, \ldots, A_m]$ e $[B_1, B_2, \ldots, B_n]$ partições de um conjunto S.

Mostre que a seguinte coleção de conjuntos é também uma partição (chamada de *partição cruzada*) de S:

$$P = [A_i \cap B_j : i = 1, \ldots, m, j = 1, \ldots, n] \setminus \emptyset$$

Observe que eliminamos o conjunto vazio $\emptyset$.

1.49 Seja $S = \{1, 2, 3, \ldots, 8, 9\}$. Determine a partição cruzada P das seguintes partições de S:

$$P_1 = [\{1, 3, 5, 7, 9\}, \{2, 4, 6, 8\}] \text{ e } P_2 = [\{1, 2, 3, 4\}, \{5, 7\}, \{6, 8, 9\}]$$

Indução

1.50 Prove: $2 + 4 + 6 + \cdots + 2n = n(n + 1)$

1.51 Prove: $1 + 4 + 7 + \cdots + 3n - 2 = \frac{n(3n-1)}{2}$

1.52 Prove: $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

1.53 Prove: $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$

1.54 Prove: $\frac{1}{1 \cdot 5} + \frac{1}{5 \cdot 9} + \frac{1}{9 \cdot 13} + \cdots + \frac{1}{(4n-3)(4n+1)} = \frac{n}{4n+1}$

1.55 Prove: $7^n - 2^n$ é divisível por 5 para todo $n \in \mathbf{N}$

1.56 Prove: $n^3 - 4n + 6$ é divisível por 3 para todo $n \in \mathbf{N}$

1.57 Use a identidade $1 + 2 + 3 + \cdots + n = n(n + 1)/2$ para provar que

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$$

Problemas variados

1.58 Suponha que $\mathbf{N} = \{1, 2, 3, \ldots\}$ é o conjunto universo e que

$$A = \{n \mid n \leq 6\}, \quad B = \{n \mid 4 \leq n \leq 9\}, \quad C = \{1, 3, 5, 7, 9\}, \quad D = \{2, 3, 5, 7, 8\}$$

Encontre: (a) $A \oplus B$; (b) $B \oplus C$; (c) $A \cap (B \oplus D)$; (d) $(A \cap B) \oplus (A \cap D)$.

1.59 Demonstre as seguintes propriedades da diferença simétrica:

(a) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$ (Associatividade)

(b) $A \oplus B = B \oplus A$ (Comutatividade)

(c) Se $A \oplus B = A \oplus C$, então $B = C$ (Cancelamento)

(d) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$ (Distributividade)

1.60 Considere m conjuntos distintos não vazios $A_1, A_2, \ldots, A_m$ em um conjunto universo **U**. Prove que:

(a) Há 2^m produtos fundamentais dos m conjuntos.

(b) Quaisquer dois produtos fundamentais são disjuntos.

(c) **U** é a união de todos os produtos fundamentais.

Respostas dos Problemas Complementares

1.26 $B = C = E = F, A = D = G = H$

1.27 $A = \{a, e, i, o, u\}, B = D = \{l, i, t, e\}$,
$C = \{a, b, c, d, e\}$

1.28 (a) C e E; (b) D e E; (c) A, B e D; (d) Nenhum.

1.29 (a) $A \cap B = \{2, 5\}, A \cap C = \{1, 5\}$;

(b) $A \cup B = \{1, 2, 5, 6, 7\}, B \cup C = \{1, 2, 3, 5, 7, 9\}$,

(c) $A^C = \{3, 4, 7, 8, 9\}, C^C = \{2, 4, 6, 8\}$;

(d) $A \backslash B = \{1, 6\}, A \backslash C = \{2, 6\}$,

(e) $A \oplus B = \{1, 6, 7\}, A \oplus C = \{2, 3, 6, 7, 9\}$;

(f) $(A \cup C) \backslash B = \{1, 3, 6, 9\}, (B \oplus C) \backslash A = \{3, 9\}$.

1.33 $A \cup B = (A^C \cap B^C)^C$.

1.34 Ver Figura 1-10.

1.35 (a) $(A \cap B \cap C) \cup (A \cap B \cap C^C) \cup (A \cap B^C \cap C)$

(b) $(A^C \cap B \cap C^C) \cup (A^C \cap B \cap C) \cup (A^C \cap B^C \cap C)$

(c) $(A \cap B \cap C) \cup (A \cap B \cap C^C) \cup (A \cap B^C \cap C)$
$\cup (A^C \cap B \cap C^C) \cup (A \cap B^C \cap C^C)$

1.36 As três premissas nos levam ao diagrama de Venn na Fig. 1-11(*a*). (a) e (b) são válidas, mas (c) não é.

1.37 (a) $A = (B^C \cup A) \cap (A \cup B)$

(b) $(A \cup B) \cap (A^C \cup B) \cap (A \cup B^C) \cap (A^C \cup B^C) = \emptyset$

1.39 (a) Infinito; (b) finito; (c) infinito; (d) finito.

1.41 Use os dados para preencher o diagrama de Venn na Fig. 1-11(*b*). Então:

(a) 5; (b) 4; (c) 2; (d) 1; (e) 6; (f) 11; (g) 23; (h) 2.

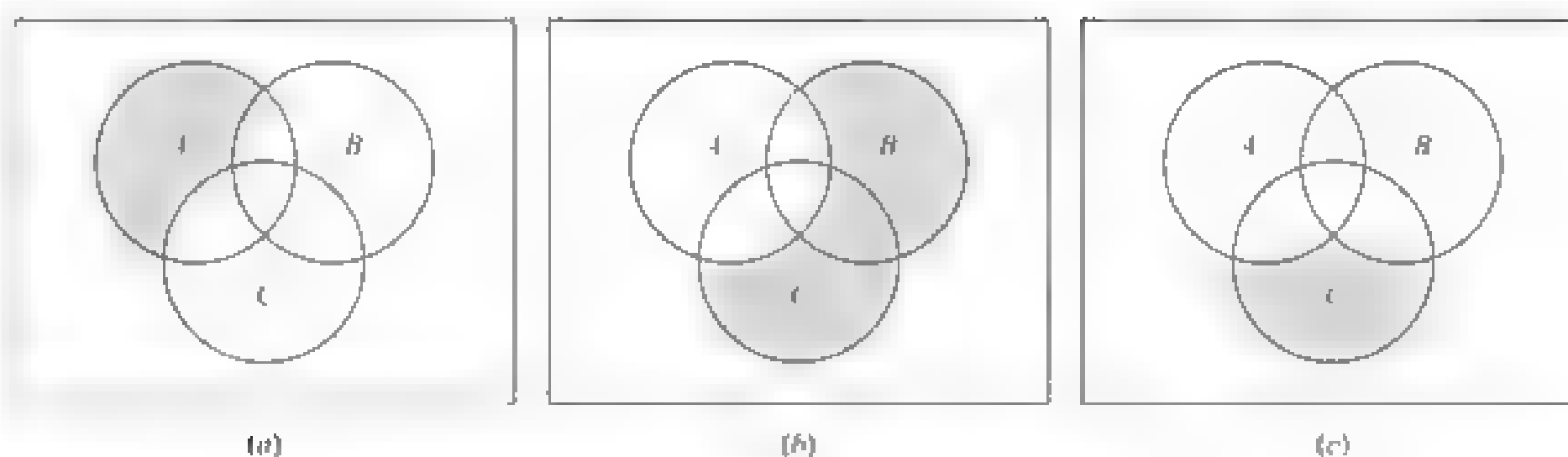



Figura 1-10

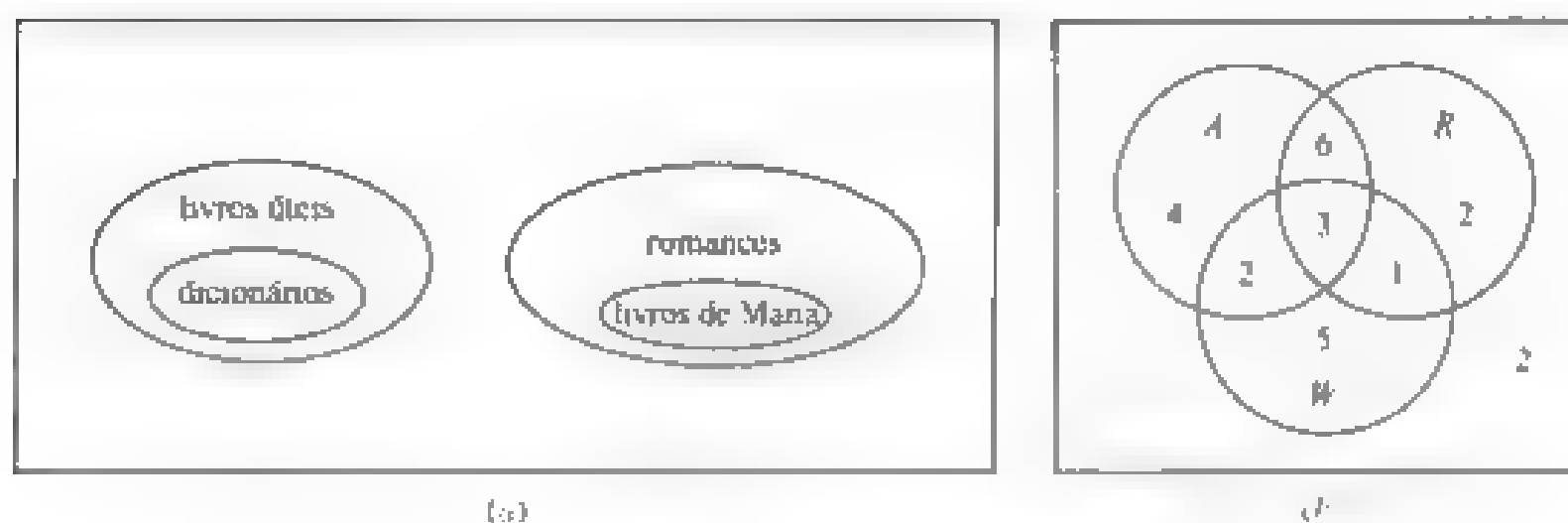



Figura 1-11

1.42 $P(A)$ tem $2^5 = 32$ elementos, como se segue:

$\{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{3, 5\}, \{4, 5\},$
$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{2, 3, 4\}, \{2, 3, 5\}, \{3, 4, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \{1, 4, 5\}, \{2, 4, 5\},$
$\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{1, 2, 4, 5\}, \{1, 3, 4, 5\}, \{2, 3, 4, 5\}, A\}$

1.43 (a) Três elementos. $\{a, b\}$, $\{c\}$ e $\{d, e, f\}$. (b) 3 (c) $P(A)$ tem $2^3 = 8$ elementos, como se segue:

$P(A) = \{A, [\{a, b\}, \{c\}], [\{a, b\}, \{d, e, f\}],$
$[\{c\}, \{d, e, f\}], [\{a, b\}], [\{c\}], [\{d, e, f\}], \emptyset\}$

1.44 Seja X um elemento em $P(A)$. Para cada $a \in A$, temos que $a \in X$ ou $a \notin X$. Como $n(A) = m$, existem 2^m conjuntos diferentes X. Ou seja, $|P(A)| = 2^m$.

1.45 (a) Não; (b) não; (c) sim; (d) sim.

1.46 (a) Não; (b) não; (c) sim; (d) não.

1.47 (a) Não; (b) não; (c) sim.

1.49 $[\{1,3\}, \{2,4\}, \{5,7\}, \{9\}, \{6,8\}]$

1.55 Sugestão: $7^{k+1} - 2^{k+1} = 7^{k+1} - 7(2^k) + 7(2^k) - 2^{k+1} = 7(7^k - 2^k) + (7 - 2)2^k$.

1.58 (a) $\{1, 2, 3, 7, 8, 9\}$; (b) $\{1, 3, 4, 6, 8\}$; (c) e (d) $\{2, 3, 4, 6\}$.

Relações

2.1 INTRODUÇÃO

O leitor está familiarizado com muitas relações, como "menor que", "é paralela a", "é um subconjunto de" e assim por diante. Em certo sentido, essas relações consideram a existência ou inexistência de uma certa conexão entre pares de objetos assumidos em uma determinada ordem. Formalmente, definimos uma relação em termos desses "pares ordenados".

Um *par ordenado* de elementos a e b, onde a é designado como o primeiro elemento e b é o segundo elemento, é denotado por (a, b). Em particular,

$$(a, b) = (c, d)$$

se, e somente se, $a = c$ e $b = d$. Portanto $(a, b) \neq (b, a)$, a menos que $a = b$. Isso contrasta com conjuntos nos quais a ordem de elementos é irrelevante; por exemplo, $\{3, 5\} = \{5, 3\}$.†

2.2 PRODUTO CARTESIANO

Considere dois conjuntos quaisquer A e B. O conjunto de todos os pares ordenados (a, b), onde $a \in A$ e $b \in B$, é chamado de *produto* ou *produto cartesiano* de A por B. Uma abreviação desse produto é $A \times B$, que se lê "A cartesiano B". Por definição,

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$$

Frequentemente, escreve-se A^2 em vez de $A \times A$.

Exemplo 2.1 $\mathbf{R}$ denota o conjunto de números reais e, assim, $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ é o conjunto de pares ordenados de números reais. O leitor está familiarizado com a representação geométrica de $\mathbf{R}^2$ na forma de pontos no plano, como na Fig. 2-1. Aqui cada ponto P representa um par ordenado (a, b) de números reais e vice-versa, a reta vertical por P encontra o eixo x em a, e a reta horizontal por P encontra o eixo y em b. $\mathbf{R}^2$ é frequentemente chamado de *plano cartesiano*.

Exemplo 2.2 Sejam $A = \{1, 2\}$ e $B = \{a, b, c\}$. Então

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$
$$B \times A = \{(a, 1), (b, 1), (c, 1), (a, 2), (b, 2), (c, 2)\}$$

Também, $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

† N. de T. Pares ordenados também podem ser definidos da seguinte maneira: $(a, b) = \{\{a\}, \{a, b\}\}$. Dessa forma (a, b) é diferente de (b, a) se, e somente se, a é diferente de b. Não há necessidade de impor artificialmente uma noção de ordem. Bastam as noções conjuntistas de pertinência e igualdade.

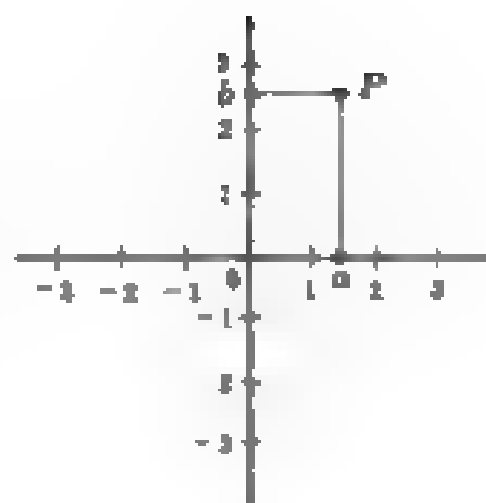



Figura 2-1

Há duas coisas que devem ser observadas nos exemplos dados. Em primeiro lugar, $A \times B \neq B \times A$. O produto cartesiano lida com pares ordenados e, assim, naturalmente a ordem na qual os conjuntos são considerados é importante. Em segundo lugar, usando $n(S)$ para o número de elementos de um conjunto, temos:

$$n(A \times B) = 6 = 2(3) = n(A)n(B)$$

De fato, $n(A \times B) = n(A)n(B)$ para quaisquer conjuntos A e B finitos. Isso decorre da observação de que, para um par ordenado (a, b) em $A \times B$, existem $n(A)$ possibilidades para a, e para cada uma dessas há $n(B)$ possibilidades para b.

A ideia de um produto de conjuntos pode ser estendida para qualquer quantia finita de conjuntos. Para quaisquer conjuntos $A_1, A_2, \ldots, A_n$, o conjunto de todas as n-uplas ordenadas $(a_1, a_2, \ldots, a_n)$, onde $a_1 \in A_1$, $a_2 \in A_2$, ..., $a_n \in A_n$, é chamado de produto dos conjuntos $A_1, \ldots, A_n$ e é denotado por

$$A_1 \times A_2 \times \cdots \times A_n \quad \text{ou} \quad \prod_{i=1}^{n} A_i$$

Assim como escrevemos A^2 no lugar de $A \times A$, também escrevemos A^n em vez de $A \times A \times \cdots \times A$, sendo que há n fatores todos iguais a A. Por exemplo, $\mathbf{R}^3 = \mathbf{R} \times \mathbf{R} \times \mathbf{R}$ denota o espaço tridimensional usual.†

2.3 RELAÇÕES

Começamos com uma definição.

Definição 2.1: Sejam A e B conjuntos. Uma *relação binária* ou, simplesmente, uma *relação* de A em B, é um subconjunto de $A \times B$.

Suponha que R é uma relação de A em B. Então R é um conjunto de pares ordenados, de modo que cada primeiro elemento vem de A e cada segundo elemento vem de B. Ou seja, para cada par $a \in A$ e $b \in B$, apenas uma das afirmações a seguir é verdadeira.

(i) $(a, b) \in R$; dizemos então que "a é R-relacionado com b", denotado como aRb.

(ii) $(a, b) \notin R$; dizemos então que "a não é R-relacionado com b", denotado como $a \not R b$.

Se R é uma relação de um conjunto A nele mesmo, isto é, se R é um subconjunto de $A^2 = A \times A$, então dizemos que R é uma relação *sobre* (ou *em*) A.

O *domínio* de uma relação R é o conjunto de todos os primeiros elementos dos pares ordenados que pertencem a R, e a *imagem* é o conjunto de segundos elementos.

Apesar de relações n-árias, que envolvem n-uplas ordenadas, serem introduzidas na Seção 2.10, o termo relação deve significar relação binária, a menos que seja estabelecido ou sugerido o contrário.

† N. de T.: Vale observar também que toda n-upla ordenada $(a_1, a_2, \ldots, a_n)$ pode ser definida como o par ordenado $((a_1, a_2, \ldots, a_{n-1}), a_n)$.

Exemplo 2.3

(a) $A = \{1, 2, 3\}$ e $B = \{x, y, z\}$, e seja $R = \{(1, y), (1, z), (3, y)\}$. Então R é uma relação de A em B, uma vez que R é um subconjunto de $A \times B$. Com respeito a essa relação,

$$1Ry,\ 1Rz,\ 3Ry, \quad \text{mas} \quad 1\not{R}x,\ 2\not{R}x,\ 2\not{R}y,\ 2\not{R}z,\ 3\not{R}x,\ 3\not{R}z$$

O domínio de R é $\{1, 3\}$ e a imagem é $\{y, z\}$.

(b) Inclusão conjuntista $\subseteq$ é uma relação sobre qualquer coleção de conjuntos. Afinal, dado qualquer par de conjuntos A e B, temos $A \subseteq B$ ou $A \not\subseteq B$.

(c) Uma relação familiar sobre o conjunto $\mathbf{Z}$ dos inteiros é "m divide n". Uma notação comum para esta relação é escrever $m|n$ quando m divide n. Portanto, $6|30$, mas $7 \nmid 25$.

(d) Considere o conjunto L de retas no plano. Perpendicularidade, escrita como "$\perp$", é uma relação sobre L. Isto é, dado qualquer par de retas a e b, temos $a \perp b$ ou $a \not\perp b$. Analogamente, "é paralela a", escrita como "$\|$", é uma relação sobre L, uma vez que $a \parallel b$ ou $a \nparallel b$.

(e) Seja A um conjunto qualquer. Uma relação importante sobre A é a de *igualdade*,

$$\{(a, a) \mid a \in A\}$$

que é geralmente denotada por "=". Essa relação é também chamada de *identidade* ou *diagonal* sobre A e é também denotada por Δ_A ou simplesmente Δ.

(f) Seja A um conjunto qualquer. Então $A \times A$ e $\emptyset$ são subconjuntos de $A \times A$ e, portanto, são relações sobre A conhecidas como *relação universal* e *relação vazia*, respectivamente.

Relação inversa

Seja R uma relação qualquer de um conjunto A em um conjunto B. A *inversa* de R, denotada por R^{-1}, é a relação de B em A que consiste nos pares ordenados tais que, quando invertidos, pertencem a R, isto é,

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}$$

Por exemplo, sejam $A = \{1, 2, 3\}$ e $B = \{x, y, z\}$. Então a inversa de

$$R = \{(1, y), (1, z), (3, y)\} \quad \text{é} \quad R^{-1} = \{(y, 1), (z, 1), (y, 3)\}$$

Claramente, se R é qualquer relação, então $(R^{-1})^{-1} = R$. Também o domínio e a imagem de R^{-1} são iguais, respectivamente, à imagem e ao domínio de R. Além disso, se R é uma relação sobre A, então R^{-1} também é uma relação sobre A.

2.4 REPRESENTAÇÕES PICTÓRICAS DE RELAÇÕES

Há várias maneiras de representar pictoricamente relações.

Relações sobre R

Seja S uma relação sobre o conjunto $\mathbf{R}$ dos números reais; isto é, S é um subconjunto de $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$. Frequentemente, S consiste em todos os pares ordenados de números reais que satisfazem alguma equação dada $E(x, y) = 0$ (tais como $x^2 + y^2 = 25$).

Como $\mathbf{R}^2$ pode ser representado pelo conjunto de pontos no plano, podemos visualizar S enfatizando aqueles pontos do plano que pertencem a S. A representação pictórica da relação é, às vezes, chamada de *gráfico* ou *grafo* da relação. Por exemplo, o gráfico da relação $x^2 + y^2 = 25$ é um círculo com centro na origem e raio 5. Ver Fig. 2-2(a).

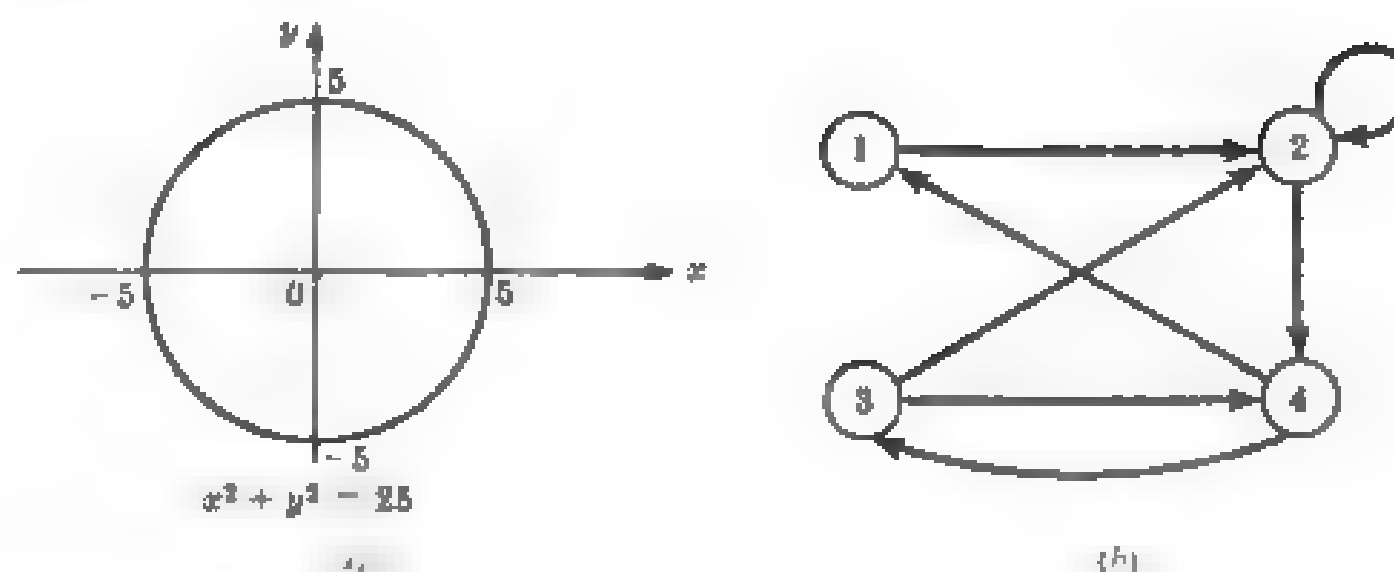



Figura 2-2

Grafos orientados de relações sobre conjuntos

Existe uma maneira importante de visualizar uma relação R em um conjunto finito. Primeiro escrevemos os elementos do conjunto e, então, desenhamos uma flecha de cada elemento x para cada elemento y, sempre que x estiver relacionado com y. Esse diagrama é chamado de grafo orientado da relação. A Fig. 2-2(*b*), por exemplo, mostra o grafo orientado da seguinte relação R sobre o conjunto $A = \{1, 2, 3, 4\}$:

$$R = \{(1, 2), (2, 2), (2, 4), (3, 2), (3, 4), (4, 1), (4, 3)\}$$

Observe que há uma flecha de 2 nele mesmo, uma vez que 2 é relacionado a 2 sob R.

Esses grafos orientados são estudados detalhadamente como um tópico separado no Capítulo 8. Mencionamos isso aqui, principalmente, para fins de completude.

Representações pictóricas de relações sobre conjuntos finitos

Suponha que A e B são conjuntos finitos. Há duas maneiras de visualizar uma relação R de A em B

(i) Formando uma disposição retangular (matricial), cujas linhas são rotuladas pelos elementos de A e cujas colunas são rotuladas pelos elementos de B. Insira um 1 ou 0 em cada posição da matriz, dependendo se $a \in A$ está relacionado ou não com $b \in B$. Essa disposição é chamada de *matriz da relação*.

(ii) Escreva os elementos de A e os elementos de B em dois discos disjuntos e, então, desenhe uma flecha de $a \in A$ a $b \in B$ sempre que a estiver relacionado com b. Essa imagem é chamada de *diagrama de flechas* da relação.

A Fig. 2-3 ilustra a relação R do Exemplo 2.3(a) por meio das duas representações acima.

$R = \{(1, y), (1, z), (3, y)\}$

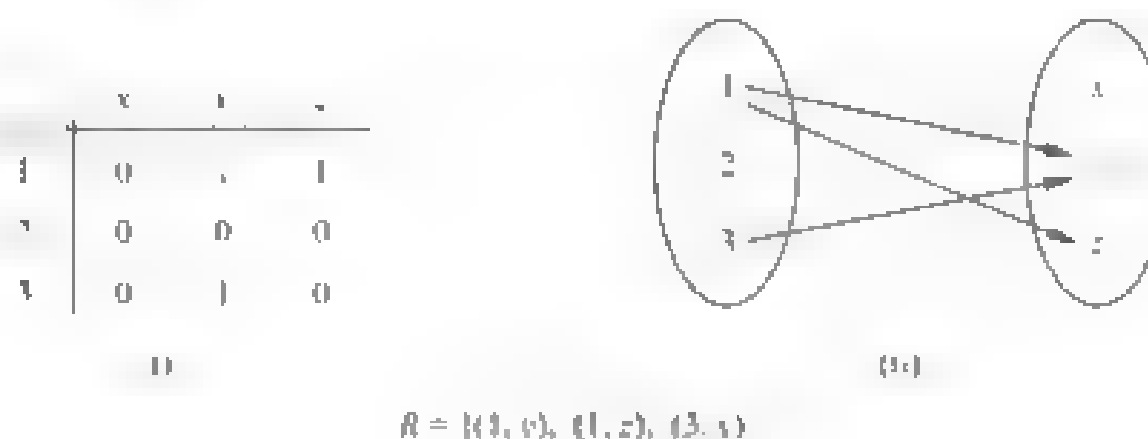



Figura 2-3

2.5 COMPOSIÇÃO DE RELAÇÕES

Sejam A, B e C conjuntos, e sejam R uma relação de A em B e S uma relação de B em C. Isto é, R é um subconjunto de $A \times B$ e S é um subconjunto de $B \times C$. Então R e S dão origem a uma relação de A em C denotada por $R \circ S$ e definida por:

$$a(R \circ S)c \text{ se, para algum } b \in B \text{, temos } aRb \text{ e } bSc.$$

Ou seja,

$$R \circ S = \{(a, c) \mid \text{existe } b \in B \text{ para o qual } (a, b) \in R \text{ e } (b, c) \in S\}$$

A relação $R \circ S$ é chamada de *composição* de R e S, às vezes, é simplesmente denotada por RS

Suponha que R é uma relação sobre um conjunto A, isto é, R é uma relação de um conjunto A nele mesmo. Então, $R \circ R$, a composição de R com ela própria, é sempre definida. Também, $R \circ R$ é eventualmente denotada por R^2. Analogamente, $R^3 = R^2 \circ R = R \circ R \circ R$, e assim por diante. Assim, R^n é definida para todo positivo n.†

Advertência: Muitos textos denotam a composição de relações R e S por $S \circ R$ em vez de $R \circ S$. Isso é feito para ficar em conformidade com o emprego usual de $g \circ f$ para denotar a composição de f e g quando estas são funções. Assim, o leitor pode ter que ajustar essa notação quando empregar este livro como complemento de outra referência bibliográfica. Contudo, quando uma relação R é composta com ela mesma, o significado de $R \circ R$ deixa de ser ambíguo.

Exemplo 2.4 Sejam $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ e $C = \{x, y, z\}$ e sejam

$$R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\} \quad \text{e} \quad S = \{(b, x), (b, z), (c, y), (d, z)\}$$

Considere os diagramas de flechas de R e S, como na Fig. 2-4. Observe que há uma flecha de 2 a d que é seguida por uma flecha de d a z. Podemos perceber essas duas flechas como um "caminho" que "conecta" o elemento $2 \in A$ ao elemento $z \in C$. Assim,

$$2(R \circ S)z, \text{ uma vez que } 2Rd \text{ e } dSz$$

Analogamente, há um caminho de 3 a x e um caminho de 3 a z. Logo,

$$3(R \circ S)x \text{ e } 3(R \circ S)z$$

Nenhum outro elemento de A está conectado a um elemento de C. Consequentemente,

$$R \circ S = \{(2, z), (3, x), (3, z)\}$$

Nosso primeiro teorema nos diz que composição de relações é associativa.

Teorema 2.1: Sejam A, B, C e D conjuntos. Suponha que R é uma relação de A a B, S é uma relação de B a C, e T é uma relação de C a D. Então

$$(R \circ S) \circ T = R \circ (S \circ T)$$

Demonstramos este teorema no Problema 2.8.

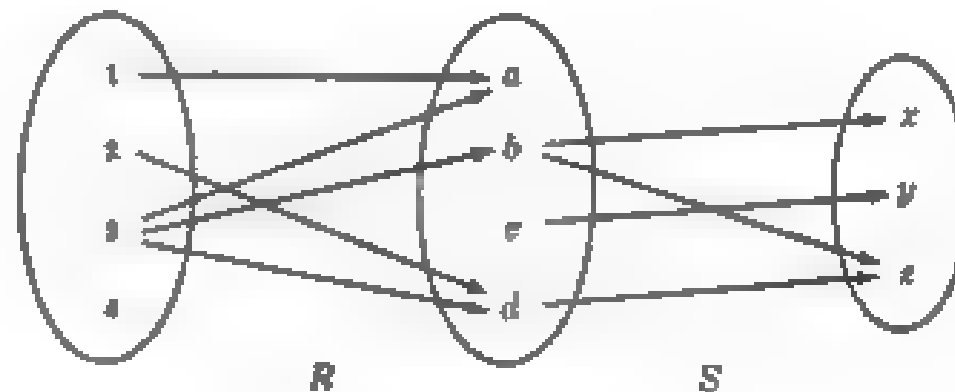



Figura 2-4

† N. de T.: Na verdade, é definida para todo inteiro positivo.

Composição de relações e matrizes

Há outra maneira de determinar $R \circ S$. Sejam M_R e M_S, respectivamente, as representações matriciais das relações R e S. Então

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{e} \quad M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

Multiplicando M_R e M_S, obtemos a matriz

$$M = M_R M_S = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

As entradas não nulas dessa matriz nos dizem quais elementos estão relacionados por $R \circ S$. Logo, $M = M_R M_S$ e $M_{R \circ S}$ têm as mesmas entradas não nulas.

2.6 TIPOS DE RELAÇÕES

Esta seção discute vários tipos importantes de relações definidas em um conjunto A.

Relações reflexivas

Uma relação R em um conjunto A é reflexiva se aRa para todo $a \in A$, isto é, se $(a, a) \in R$ para todo $a \in A$. Portanto, R não é reflexiva se existe $a \in A$ tal que $(a, a) \notin R$.

Exemplo 2.5 Considere as cinco relações a seguir sobre o conjunto $A = \{1, 2, 3, 4\}$:

$$R_1 = \{(1, 1), (1, 2), (2, 3), (1, 3), (4, 4)\}$$
$$R_2 = \{(1, 1)(1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$$
$$R_3 = \{(1, 3), (2, 1)\}$$
$$R_4 = \emptyset, \text{ a relação vazia}$$
$$R_5 = A \times A, \text{ a relação universal}$$

Determine quais das relações são reflexivas.

Como A tem os quatro elementos 1, 2, 3 e 4, uma relação R em A é reflexiva se tiver os quatro pares $(1, 1)$, $(2, 2)$, $(3, 3)$ e $(4, 4)$. Assim, apenas R_2 e a relação universal $R_5 = A \times A$ são reflexivas. Note que R_1, R_3 e R_4 não são reflexivas, pois, por exemplo, $(2, 2)$ não pertence a qualquer uma delas.

Exemplo 2.6 Considere as cinco relações a seguir:

(1) Relação $\leq$ (menor ou igual) sobre o conjunto $\mathbf{Z}$ dos inteiros.

(2) Inclusão conjuntista $\subseteq$ sobre uma coleção C de conjuntos.

(3) Relação $\perp$ (perpendicular) sobre o conjunto L de retas no plano.

(4) Relação $\parallel$ (paralela) sobre o conjunto L de retas no plano.

(5) Relação $|$ de divisibilidade sobre o conjunto $\mathbf{N}$ de inteiros positivos. (Lembre que $x \mid y$ se existe z tal que $xz = y$.)

Determine quais das relações são reflexivas.

A relação (3) não é reflexiva, uma vez que nenhuma reta é perpendicular a ela mesma. Também (4) é não reflexiva, pois nenhuma reta é paralela a ela própria. As demais relações são reflexivas; ou seja, $x \leq x$ para todo $x \in \mathbf{Z}$, $A \subseteq A$ para qualquer conjunto $A \in C$, e $n \mid n$ para todo inteiro positivo $n \in \mathbf{N}$

Relações simétricas e antissimétricas

Uma relação R sobre um conjunto A é *simétrica* se aRb implica bRa, isto é, sempre que tivermos $(a, b) \in R$, então $(b, a) \in R$. Assim, R não é simétrica se existirem $a, b \in A$ tais que $(a, b) \in R$, mas $(b, a) \notin R$.

Exemplo 2.7

(a) Determine quais das relações do Exemplo 2.5 são simétricas.

R_1 não é simétrica, uma vez que $(1, 2) \in R_1$, mas $(2, 1) \notin R_1$. R_3 não é simétrica, pois $(1, 3) \in R_3$, mas $(3, 1) \notin R_3$. As outras relações são simétricas.

(b) Determine quais das relações do Exemplo 2.6 são simétricas.

A relação $\perp$ é simétrica, pois se a reta a é perpendicular à reta b, então b é perpendicular a a. Também $\parallel$ é simétrica, uma vez que, se a reta a é paralela à reta b, então b é paralela a a. As demais relações não são simétricas. Por exemplo:

$$3 \leq 4 \text{ mas } 4 \not\leq 3; \quad \{1, 2\} \subseteq \{1, 2, 3\} \text{ mas } \{1, 2, 3\} \not\subseteq \{1,2\}; \quad \text{e} \quad 2 \mid 6 \text{ mas } 6 \nmid 2.$$

Uma relação R sobre um conjunto A é *antissimétrica* se aRb e bRa implicarem que $a = b$; ou seja, se $a \neq b$ e aRb, então $b\not{R}a$. Logo, R não é antissimétrica se existirem elementos distintos a e b em A tais que aRb e bRa.

Exemplo 2.8

(a) Determine quais das relações do Exemplo 2.5 são antissimétricas.

R_2 não é antissimétrica, pois $(1, 2)$ e $(2, 1)$ pertencem a R_2, mas $1 \neq 2$. Analogamente, a relação universal R_5 não é antissimétrica. Todas as demais relações são antissimétricas

(b) Determine quais das relações do Exemplo 2.6 são antissimétricas.

A relação $\leq$ é antissimétrica, uma vez que $a \leq b$ e $b \leq a$ implicam que $a = b$. A inclusão conjuntista $\subseteq$ é antissimétrica, pois sempre que $A \subset B$ e $B \subset A$, temos $A = B$. Também, divisibilidade sobre $\mathbf{N}$ é antissimétrica, uma vez que $m \mid n$ e $n \mid m$ implicam $m = n$. (Note que divisibilidade sobre $\mathbf{Z}$ não é antissimétrica, pois $3 \mid -3$ e $-3 \mid 3$, mas $3 \neq -3$.) As relações $\perp$ e $\parallel$ não são antissimétricas.

Observação: As propriedades de simetria e antissimetria não são negações uma da outra. Por exemplo, a relação $R = \{(1, 3), (3, 1), (2, 3)\}$ não é simétrica nem antissimétrica. Por outro lado, a relação $R' = \{(1, 1), (2, 2)\}$ é simétrica e antissimétrica.

Relações transitivas

Uma relação R sobre um conjunto A é *transitiva* se aRb e bRc implicarem aRc, isto é, sempre que $(a, b), (b, c) \in R$, então $(a, c) \in R$. Assim, R não é transitiva se existirem $a, b, c \in R$ tais que $(a, b), (b, c) \in R$, mas $(a, c) \notin R$

Exemplo 2.9

(a) Determine quais das relações no Exemplo 2.5 são transitivas.

A relação R_3 não é transitiva, pois $(2, 1), (1, 3) \in R_3$, mas $(2, 3) \notin R_3$. Todas as outras relações são transitivas.

(b) Determine quais das relações do Exemplo 2.6 são transitivas.

As relações $<$, $\subset$ e , são transitivas, mas certamente não $\perp$. Também, como nenhuma reta é paralela a si mesma, podemos ter $a \parallel b$ e $b \parallel a$, mas $a \nparallel a$. Assim, $\parallel$ não é transitiva. (Observamos que a relação "é paralela ou igual a" é transitiva sobre o conjunto L de retas do plano.)

A propriedade de transitividade pode também ser expressa em termos da composição de relações. Para uma relação R sobre A, definimos $R^2 = R \circ R$ e, no caso geral, $R^n = R^{n-1} \circ R$. Então, temos o seguinte resultado:

Teorema 2.2: Uma relação R é transitiva se, e somente se, para todo $n \geq 1$ temos $R^n \subseteq R$.

2.7 PROPRIEDADES DE FECHO

Considere um dado conjunto A e a coleção de todas as relações sobre A. Seja P uma propriedade de tais relações, como simetria ou transitividade. Uma relação com a propriedade P será chamada de P-relação. O P-fecho de uma relação arbitrária R sobre A, escrito como $P(R)$, é uma P-relação tal que

$$R \subseteq P(R) \subseteq S$$

para cada P-relação S contendo R. Escrevemos

$$\text{reflexiva}(R), \quad \text{simétrica}(R) \quad \text{e} \quad \text{transitiva}(R)$$

para os fechos reflexivo, simétrico e transitivo de R.

Em termos gerais, $P(R)$ não precisa existir. No entanto, há uma situação geral na qual $P(R)$ sempre existirá. Suponha que P é uma propriedade tal que exista pelo menos uma P-relação contendo R e que a interseção de quaisquer P-relações seja novamente uma P-relação. Então, pode-se provar (Problema 2.12) que

$$P(R) = \cap (S \mid S \text{ é uma } P\text{-relação e } R \subseteq S)$$

Assim, pode-se obter $P(R)$ a partir da "queda", ou seja, como a interseção de relações. No entanto, geralmente queremos encontrar $P(R)$ a partir da "subida", ou seja, acrescentando elementos a R para obter $P(R)$. Isso será mostrado a seguir.

Fechos reflexivo e simétrico

O próximo teorema nos diz como facilmente obter os fechos reflexivo e simétrico de uma relação. Aqui $\Delta_A = \{(a, a) \mid a \in A\}$ é a diagonal ou relação de igualdade sobre A.

Teorema 2.3: Seja R uma relação sobre um conjunto A. Então:

(i) $R \cup \Delta_A$ é o fecho reflexivo de R.

(ii) $R \cup R^{-1}$ é o fecho simétrico de R.

Em outras palavras, a reflexiva(R) é obtida simplesmente adicionando a R aqueles elementos (a, a) da diagonal que não pertenciam a R, e a simétrica(R) é conseguida acrescentando a R todos os pares (b, a) sempre que (a, b) pertencer a R.

Exemplo 2.10 Considere a relação $R = \{(1, 1), (1, 3), (2, 4), (3, 1), (3, 3), (4, 3)\}$ sobre o conjunto $A = \{1, 2, 3, 4\}$. Então

$$\text{reflexiva}(R) = R \cup \{(2, 2), (4, 4)\} \quad \text{e} \quad \text{simétrica}(R) = R \cup \{(4, 2), (3, 4)\}$$

Fecho transitivo

Seja R uma relação sobre um conjunto A. Lembre que $R^2 = R \circ R$ e $R^n = R^{n-1} \circ R$. Definimos

$$R^* = \bigcup_{i=1}^{\infty} R^i$$

O teorema a seguir se aplica:

Teorema 2.4: R^* é o fecho transitivo de R

Suponha que A é um conjunto finito com n elementos. Mostramos no Capítulo 8 sobre grafos que

$$R^* = R \cup R^2 \cup \ldots \cup R^n$$

Isso nos dá o seguinte teorema.

Teorema 2.5: Seja R uma relação sobre um conjunto A com n elementos. Então

$$\text{transitiva } (R) = R \cup R^2 \cup \ldots \cup R^n$$

Exemplo 2.11 Considere a relação $R = \{(1, 2), (2, 3), (3, 3)\}$ sobre $A = \{1, 2, 3\}$. Então:

$$R^2 = RoR = \{(1, 3), (2, 3), (3, 3)\} \quad \text{e} \quad R^3 = R^2oR = \{(1, 3), (2, 3), (3, 3)\}$$

Consequentemente,

$$\text{transitiva } (R) = \{(1, 2), (2, 3), (3, 3), (1, 3)\}$$

2.8 RELAÇÕES DE EQUIVALÊNCIA

Considere um conjunto S não vazio. Uma relação R sobre S é uma *relação de equivalência* se R é reflexiva, simétrica e transitiva. Ou seja, R é uma relação de equivalência sobre S se tiver as três propriedades a seguir:

(1) Para todo $a \in S$, aRa. (2) Se aRb, então bRa. (3) Se aRb e bRc, então aRc.

A ideia geral por trás de uma relação de equivalência é a de que se trata de uma classificação de objetos que são, de algum modo, "semelhantes". De fato, a relação "=" de igualdade sobre qualquer conjunto S é uma relação de equivalência; ou seja,

(1) $a = a$ para todo $a \in S$. (2) Se $a = b$, então $b = a$. (3) Se $a = b$, $b = c$, então $a = c$

Outras relações de equivalência se seguem.

Exemplo 2.12

(a) Sejam L o conjunto de retas e T o conjunto de triângulos no plano euclidiano.

  (i) A relação "é paralela ou igual a" é uma relação de equivalência sobre L.

  (ii) As relações de congruência e semelhança são relações de equivalência sobre T.

(b) A relação $\subseteq$ de inclusão conjuntista não é de equivalência. Ela é reflexiva e transitiva, mas não é simétrica, uma vez que $A \subseteq B$ não implica que $B \subseteq A$.

(c) Seja m um inteiro positivo fixo. Dois inteiros a e b são ditos *congruentes módulo m*, o que se denota como

$$a \equiv b \pmod{m}$$

se m divide $a - b$. Por exemplo, para o módulo $m = 4$, temos

$$11 \equiv 3 (\text{mod } 4) \quad \text{e} \quad 22 \equiv 6 \ (\text{mod } 4)$$

pois 4 divide $11 - 3 = 8$ e 4 divide $22 - 6 = 16$. Essa relação de congruência módulo m é uma relação de equivalência importante.

Relações de equivalência e partições

Esta subseção explora a relação entre relações de equivalência e partições em um conjunto não vazio S. Lembre que uma partição P de S é uma coleção $\{A_i\}$ de subconjuntos não vazios de S com as duas propriedades a seguir:

(1) Cada $a \in S$ pertence a algum A_i.

(2) Se $A_i \neq A_j$, então $A_i \cap A_j = \emptyset$.

Em outras palavras, uma partição P de S é uma subdivisão de S em conjuntos disjuntos e não vazios. (Ver Seção 1.7.)

Suponha que R é uma relação de equivalência em um conjunto S. Para cada $a \in S$, seja $[a]$ o conjunto de elementos de S que estão relacionados com a por R; isto é:

$$[a] = \{x \mid (a, x) \in R\}$$

Chamamos $[a]$ de *classe de equivalência* de a em S; qualquer $b \in [a]$ é dito um *representante* da classe de equivalência.

A coleção de todas as classes de equivalência de elementos de S, relativamente a uma relação de equivalência R, é denotada por S/R, ou seja,

$$S/R = \{[a] \mid a \in S\}$$

Ela é chamada de *conjunto quociente* de S por R. A propriedade fundamental de um conjunto quociente está contida no teorema a seguir.

Teorema 2.6: Seja R uma relação de equivalência em um conjunto S. Então S/R é uma partição de S. Especificamente:

(i) Para cada a em S, temos $a \in [a]$.

(ii) $[a] = [b]$ se, e somente se, $(a, b) \in R$.

(iii) Se $[a] \neq [b]$, então $[a]$ e $[b]$ são disjuntos.

Reciprocamente, dada uma partição $\{A_i\}$ do conjunto S, existe uma relação de equivalência R em S tal que os conjuntos A_i são as classes de equivalência.

Esse importante teorema é demonstrado no Problema 2.17.

Exemplo 2.13

(a) Considere a relação $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$ em $S = \{1, 2, 3\}$.

Pode-se mostrar que R é reflexiva, simétrica e transitiva, ou seja, que R é uma relação de equivalência. Também:

$$[1] = \{1, 2\}, [2] = \{1, 2\}, [3] = \{3\}$$

Observe que $[1] = [2]$ e que $S/R = \{[1], [3]\}$ é uma partição de S. Podemos escolher $\{1, 3\}$ ou $\{2, 3\}$ como um conjunto de representantes das classes de equivalência.

(b) Seja R_5 a relação de congruência módulo 5 sobre o conjunto $\mathbf{Z}$ dos inteiros, denotada por

$$x \equiv y \pmod 5$$

Isso significa que a diferença $x - y$ é divisível por 5. Então R_5 é uma relação de equivalência sobre $\mathbf{Z}$. O conjunto quociente $\mathbf{Z}/R_5$ contém as cinco classes de equivalência a seguir:

$$\begin{aligned} A_0 &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\ A_1 &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\ A_2 &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\ A_3 &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\ A_4 &= \{\ldots, -6, -1, 4, 9, 14, \ldots\} \end{aligned}$$

Qualquer inteiro x, unicamente expresso na forma $x = 5q + r$, onde $0 < r < 5$, é um membro da classe de equivalência A_r, sendo r o resto. Como o esperado, $\mathbf{Z}$ é a união disjunta das classes de equivalência A_0, A_1, A_2, A_3 e A_4. Geralmente se escolhe $\{0, 1, 2, 3, 4\}$ ou $\{-2, -1, 0, 1, 2\}$ como um conjunto de representantes das classes de equivalência.

2.9 RELAÇÕES DE ORDEM PARCIAL

Uma relação R sobre um conjunto S é chamada de *ordem parcial* de S se R é reflexiva, antissimétrica e transitiva. Um conjunto S munido de uma relação de ordem parcial R é dito um *conjunto parcialmente ordenado*. Conjuntos parcialmente ordenados são estudados detalhadamente no Capítulo 14. Portanto, apresentamos aqui apenas alguns exemplos.

Exemplo 2.14

(a) A relação $\subseteq$ de inclusão conjuntista é uma ordem parcial sobre qualquer coleção de conjuntos, uma vez que a inclusão conjuntista tem as três propriedades desejadas. Ou seja,

 (1) $A \subseteq A$ para qualquer conjunto A

 (2) Se $A \subseteq B$ e $B \subseteq A$, então $A = B$

 (3) Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

(b) A relação $\leq$ sobre o conjunto $\mathbf{R}$ dos números reais é reflexiva, antissimétrica e transitiva. Assim, $\leq$ é uma ordem parcial em $\mathbf{R}$.

(c) A relação "a divide b", escrita como $a \mid b$, é uma ordem parcial sobre o conjunto $\mathbf{N}$ dos inteiros positivos. Contudo, "a divide b" não é uma ordem parcial sobre o conjunto $\mathbf{Z}$ dos inteiros, uma vez que $a \mid b$ e $b \mid a$ não implicam $a = b$. Por exemplo, $3 \mid -3$ e $-3 \mid 3$, mas $3 \neq -3$.

2.10 RELAÇÕES n-ÁRIAS

Todas as relações recém discutidas são binárias. Por uma *relação* n-*ária*, queremos dizer um conjunto de n-uplas ordenadas. Para qualquer conjunto S, um subconjunto do produto cartesiano S^n é dito uma relação n-ária sobre S. Especificamente, um subconjunto de S^3 é denominado uma *relação ternária* sobre S.

Exemplo 2.15

(a) Seja L uma reta no plano. Então "estar entre" é uma relação ternária R sobre os pontos de L; ou seja, $(a, b, c) \in R$ se b está entre a e c em L.

(b) A equação $x^2 + y^2 + z^2 = 1$ determina uma relação ternária T sobre o conjunto $\mathbf{R}$ dos números reais. Isto é, uma tripla (x, y, z) pertence a T se (x, y, z) satisfaz a equação, o que significa que (x, y, z) são as coordenadas de um ponto em $\mathbf{R}^3$ sobre a esfera S de raio 1 e centro na origem $O = (0, 0, 0)$.

Problemas Resolvidos

Produto cartesiano

2.1 Dados $A = \{1, 2\}$, $B = \{x, y, z\}$ e $C = \{3, 4\}$, determine $A \times B \times C$.

$A \times B \times C$ consiste em todas as triplas ordenadas (a, b, c), onde $a \in A$, $b \in B$ e $c \in C$. Esses elementos de $A \times B \times C$ podem ser sistematicamente obtidos por um diagrama em árvore (Fig. 2-5). Os elementos de $A \times B \times C$ são precisamente as 12 triplas ordenadas à direita do diagrama em árvore.

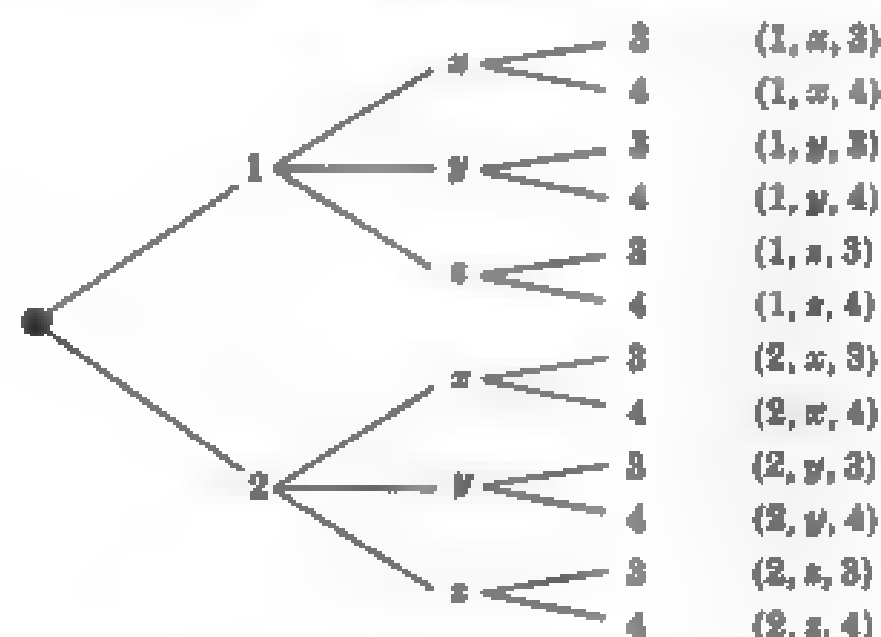



Figura 2-5

Observe que $n(A) = 2$, $n(B) = 3$ e $n(C) = 2$ e, como o esperado,

$$n(A \times B \times C) = 12 = n(A) \cdot n(B) \cdot n(C)$$

2.2 Encontre x e y, dado $(2x, x + y) = (6, 2)$.

Dois pares ordenados são iguais se, e somente se, as componentes correspondentes são iguais. Logo, obtemos as equações

$$2x = 6 \quad \text{e} \quad x + y = 2$$

a partir das quais obtemos as respostas $x = 3$ e $y = -1$

Relações e seus grafos

2.3 Determine o número de relações de $A = \{a, b, c\}$ em $B = \{1, 2\}$.

Há $3(2) = 6$ elementos em $A \times B$ e, portanto, existem $m = 2^6 = 64$ subconjuntos de $A \times B$. Logo, há $m = 64$ relações de A em B

2.4 Sejam $A = \{1, 2, 3, 4\}$ e $B = \{x, y, z\}$. Seja R a seguinte relação de A em B:

$$R = \{(1, y), (1, z), (3, y), (4, x), (4, z)\}$$

(a) Determine a matriz da relação.

(b) Esboce o diagrama de flechas de R

(c) Encontre a relação inversa R^{-1} de R

(d) Determine o domínio e a imagem de R

(a) Veja a Fig. 2-6(a). Observe que as linhas da matriz são rotuladas pelos elementos de A e as colunas pelos elementos de B. Também note que a entrada na matriz correspondente a $a \in A$ e $b \in B$ é 1 se a se relaciona com b e 0 no caso contrário.

(b) Veja a Fig. 2-6(b). Observe que há uma flecha de $a \in A$ a $b \in B$ se, e somente se, a se relaciona com b, ou seja, se $(a, b) \in R$.

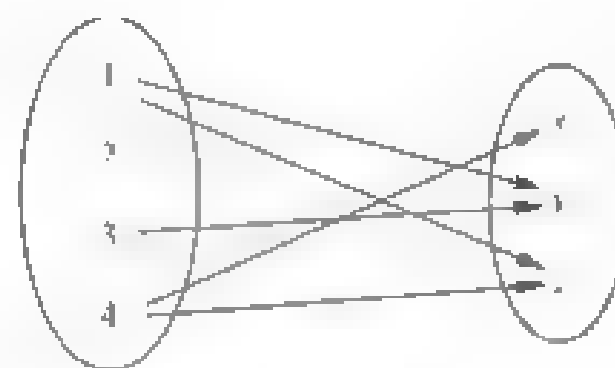



Figura 2-6

(c) Inverta os pares ordenados de R para obter R^{-1}:

$$R^{-1} = \{(y, 1), (z, 1), (y, 3), (x, 4), (z, 4)\}$$

Note que, invertendo as flechas na Fig. 2-6(b), obtemos o diagrama em flechas de R^{-1}.

(d) O domínio de R, Dom(R), consiste nos primeiros elementos dos pares ordenados de R, e a imagem de R, Im(R), é formada pelos segundos elementos. Logo,

$$\text{Dom}(R) = \{1, 3, 4\} \text{ e } \text{Im}(R) = \{x, y, z\}$$

2.5 Sejam $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ e $C = \{x, y, z\}$. Considere as seguintes relações R e S de A em B e de B em C, respectivamente.

$$R = \{(1, b), (2, a), (2, c)\} \quad \text{e} \quad S = \{(a, y), (b, x), (c, y), (c, z)\}$$

(a) Encontre a relação de composição $R \circ S$

(b) Encontre as matrizes M_R, M_S e $M_{R \circ S}$ das respectivas relações R, S e $R \circ S$ e compare $M_{R \circ S}$ com o produto $M_R M_S$.

(a) Esboce o diagrama em flechas das relações R e S, como na Fig. 2-7(a). Observe que 1 em A está "conectado" a x em C pelo caminho $1 \to b \to x$; logo, $(1, x)$ pertence a $R \circ S$. Analogamente, $(2, y)$ e $(2, z)$ pertencem a $R \circ S$.

Temos

$$R \circ S = \{(1, x), (2, y), (2, z)\}$$

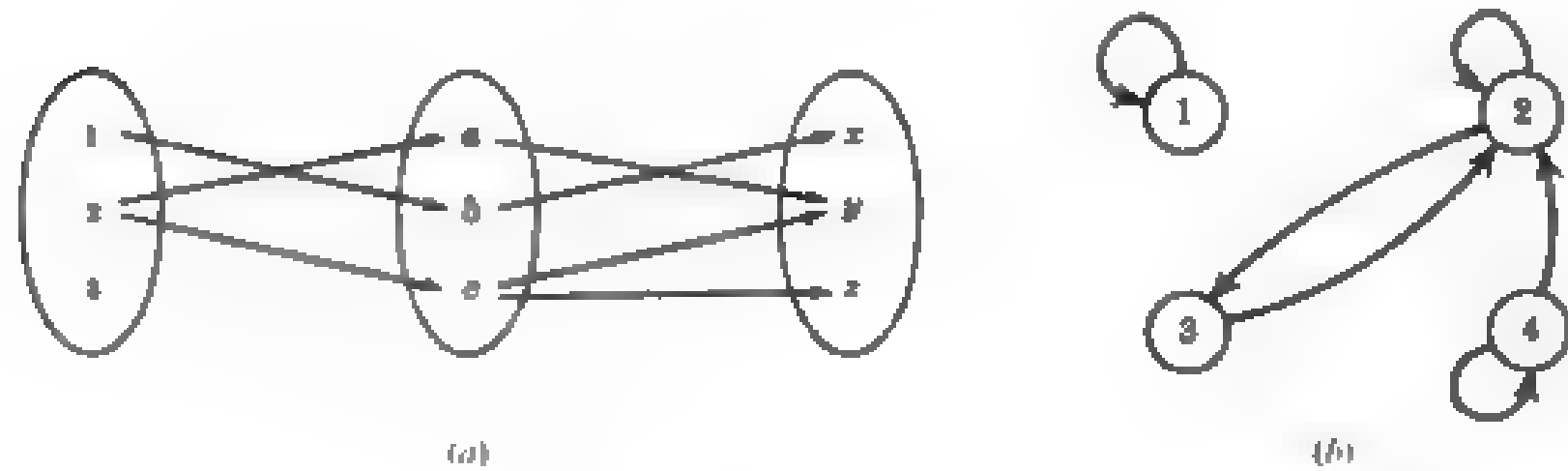



Figura 2-7

(b) As matrizes de M_R, M_S e $M_{R \circ S}$ seguem abaixo:

$$M_R = \begin{matrix} & a & b & c \\ 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \\ 3 & 0 & 0 & 0 \end{matrix} \qquad M_S = \begin{matrix} & x & y & z \\ a & 0 & 1 & 0 \\ b & 1 & 0 & 0 \\ c & 0 & 1 & 1 \end{matrix} \qquad M_{R \circ S} = \begin{matrix} & x & y & z \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 1 \\ 3 & 0 & 0 & 0 \end{matrix}$$

Multiplicando M_R por M_S, obtemos

$$M_R M_S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Observe que $M_{R \circ S}$ e $M_R M_S$ têm as mesmas entradas nulas.

2.6 Considere a relação $R = \{(1, 1), (2, 2), (2, 3), (3, 2), (4, 2), (4, 4)\}$ sobre $A = \{1, 2, 3, 4\}$

(a) Esboce seu grafo orientado. (b) Determine $R^2 = R \circ R$

(a) Para cada $(a, b) \in R$, esboce uma flecha de a em b, como na Fig. 2-7(b).

(b) Para cada par $(a, b) \in R$, encontre todos os $(b, c) \in R$. Então $(a, c) \in R^2$. Logo,

$$R^2 = \{(1, 1), (2, 2), (2, 3), (3, 2), (3, 3), (4, 2), (4, 3), (4, 4)\}$$

2.7 Sejam R e S as seguintes relações em $A = \{1, 2, 3\}$.

$$R = \{(1, 1), (1, 2), (2, 3), (3, 1), (3, 3)\}, \quad S = \{(1, 2), (1, 3), (2, 1), (3, 3)\}$$

Encontre (a) $R \cup S$, $R \cap S$, R^C; (b) $R \circ S$; (c) $S^2 = S \circ S$.

(a) Considere R e S simplesmente como conjuntos e faça a interseção e união usuais. Para R^C, usamos o fato de que $A \times A$ é a relação universal sobre A.

$$R \cap S = \{(1, 2), (3, 3)\}$$
$$R \cup S = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\}$$
$$R^C = \{(1, 3), (2, 1), (2, 2), (3, 2)\}$$

(b) Para cada par $(a, b) \in R$, determine todos os pares $(b, c) \in S$. Então, $(a, c) \in R \circ S$. Por exemplo, $(1,1) \in R$ e $(1, 2)$, $(1, 3) \in S$; logo, $(1, 2)$ e $(1, 3)$ pertencem a $R \circ S$. Assim,

$$R \circ S = \{(1, 2), (1, 3), (1, 1), (2, 3), (3, 2), (3, 3)\}$$

(c) Segundo o algoritmo em (b), temos

$$S^2 = S \circ S = \{(1, 1), (1, 3), (2, 2), (2, 3), (3, 3)\}$$

2.8 Prove o Teorema 2.1. Sejam A, B, C e D conjuntos. Suponha que R é uma relação de A em B, S é uma relação de B em C e T é uma relação de C em D. Então $(R \circ S) \circ T = R \circ (S \circ T)$.

Precisamos mostrar que cada par ordenado em $(R \circ S) \circ T$ pertence a $R \circ (S \circ T)$ e vice-versa.

Suponha que (a, d) pertence a $(R \circ S) \circ T$. Então, existe $c \in C$ tal que $(a, c) \in R \circ S$ e $(c, d) \in T$. Como $(a, c) \in R \circ S$, existe $b \in B$ tal que $(a, b) \in R$ e $(b, c) \in S$. Uma vez que $(b, c) \in S$ e $(c, d) \in T$, temos $(b, d) \in S \circ T$; e, uma vez que $(a, b) \in R$ e $(b, d) \in S \circ T$, temos $(a, d) \in R \circ (S \circ T)$. Portanto, $(R \circ S) \circ T \subset R \circ (S \circ T)$. Analogamente, $R \circ (S \circ T) \subset (R \circ S) \circ T$. Ambas as inclusões de relações provam que $(R \circ S) \circ T = R \circ (S \circ T)$.

Tipos de relações e propriedades de fecho

2.9 Considere as cinco relações a seguir sobre o conjunto $A = \{1, 2, 3\}$.

$R = \{(1, 1), (1, 2), (1, 3), (3, 3)\}$, $\emptyset$ = relação vazia

$S = \{(1, 1)(1, 2), (2, 1)(2, 2), (3, 3)\}$, $A \times A$ = relação universal

$T = \{(1, 1), (1, 2), (2, 2), (2, 3)\}$

Determine se cada uma das relações acima sobre A é: (a) reflexiva, (b) simétrica; (c) transitiva, (d) antissimétrica.

(a) R não é reflexiva, uma vez que $2 \in A$, mas $(2, 2) \notin R$. T não é reflexiva, pois $(3, 3) \notin T$ e, analogamente, $\emptyset$ não é reflexiva. S e $A \times A$ são reflexivas.

(b) R não é simétrica, uma vez que $(1, 2) \in R$, mas $(2, 1) \notin R$, e, analogamente, T não é simétrica. S, $\emptyset$, e $A \times A$ são simétricas.

(c) T não é transitiva, uma vez que $(1, 2)$ e $(2, 3)$ pertencem a T, mas $(1, 3)$ não pertence. As outras quatro relações são transitivas.

(d) S não é antissimétrica, uma vez que $1 \neq 2$ e $(1, 2)$ e $(2, 1)$ pertencem a S. Analogamente, $A \times A$ não é antissimétrica. As outras três relações são antissimétricas.

2.10 Dê um exemplo de uma relação R em $A = \{1, 2, 3\}$ tal que:

(a) R é simétrica e antissimétrica.

(b) R não é simétrica nem antissimétrica.

(c) R é transitiva, mas $R \cup R^{-1}$ não é.

Há vários exemplos. Uma coleção possível de exemplos segue abaixo:

(a) $R = \{(1, 1), (2, 2)\}$, (b) $R = \{(1, 2), (2, 1), (2, 3)\}$, (c) $R = \{(1, 2)\}$.

2.11 Suponha que C é uma coleção de relações S sobre um conjunto A, e seja T a interseção das relações S em C, ou seja, $T = \cap (S \mid S \in C)$. Prove que:

(a) Se toda S é simétrica, então T é simétrica.

(b) Se toda S é transitiva, então T é transitiva.

(a) Suponha que $(a, b) \in T$. Então, $(a, b) \in S$ para toda S. Como cada S é simétrica, $(b, a) \in S$ para toda S. Logo, $(b, a) \in T$ e T é simétrica.

(b) Suponha que (a, b) e (b, c) pertençam a T. Então, (a, b) e (b, c) pertencem a S para toda S. Como cada S é transitiva, (a, c) pertence a S para cada S. Logo, $(a, c) \in T$ e T é transitiva.

2.12 Seja R uma relação sobre um conjunto A, e seja P uma propriedade sobre relações, como simetria e transitividade. Então P é chamada de *R-fechável* se P satisfaz as duas condições a seguir

(1) Há uma P-relação S contendo R

(2) A interseção de P-relações é uma P-relação.

(a) Mostre que simetria e transitividade são R-fecháveis para qualquer relação R.

(b) Suponha que P é R-fechável. Então $P(R)$, o P-fecho de R, é a interseção de todas as P-relações S contendo R, ou seja,

$$P(R) = \cap(S \mid S \text{ é uma } P\text{-relação e } R \subseteq S)$$

(a) A relação universal $A \times A$ é simétrica e transitiva e $A \times A$ contém qualquer relação R em A. Assim, (1) é satisfeita. Pelo Problema 2.11, simetria e transitividade satisfazem (2). Logo, simetria e transitividade são R-fecháveis para qualquer relação R

(b) Seja $T = \cap(S \mid S$ é uma P-relação e $R \subseteq S)$. Como P é R-fechável, T é não vazia, por (1), e T é uma P-relação, por (2). Como cada relação S contém R, a interseção T contém R. Assim, T é uma P-relação contendo R. Por definição, $P(R)$ é a menor P-relação contendo R, logo, $P(R) \subseteq T$. Por outro lado, $P(R)$ é um dos conjuntos S definindo T, isto é, $P(R)$ é uma P-relação e $R \subseteq P(R)$. Portanto, $T \subseteq P(R)$. Consequentemente, $P(R) = T$.

2.13 Considere a relação $R = \{(a, a), (a, b), (b, c), (c, c)\}$ sobre o conjunto $A = \{a, b, c\}$. Encontre (a) reflexiva(R); (b) simétrica(R); (c) transitiva(R).

(a) O fecho reflexivo sobre R é obtido, acrescentando-se todos os pares diagonais de $A \times A$ em R que não estão presentes em R. Logo,

$$\text{reflexiva}(R) = R \cup \{(b, b)\} = \{(a, a), (a, b), (b, b), (b, c), (c, c)\}$$

(b) O fecho simétrico sobre R é obtido, acrescentando-se todos os pares de R^{-1} em R que não estão presentes em R. Portanto,

$$\text{simétrica}(R) = R \cup \{(b, a), (c, b)\} = \{(a, a), (a, b), (b, a), (b, c), (c, b), (c, c)\}$$

(c) O fecho transitivo em R, como A tem três elementos, é obtido fazendo-se a união de R com $R^2 = RoR$ e $R^3 = RoRoR$. Observe que

$$R^2 = RoR = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$
$$R^3 = RoRoR = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

Logo,

$$\text{transitiva}(R) = R \cup R^2 \cup R^3 = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

Relações de equivalência e partições

2.14 Considere o **Z** dos inteiros e um inteiro $m > 1$. Dizemos que x é congruente a y módulo m, que se denota como

$$x \equiv y \pmod{m}$$

se $x - y$ é divisível por m. Mostre que isso define uma relação de equivalência sobre **Z**.

Devemos mostrar que a relação é reflexiva, simétrica e transitiva.

(i) Para qualquer x em Z, temos $x \equiv x \pmod{m}$, pois $x - x = 0$ é divisível por m. Logo, a relação é reflexiva.

(ii) Suponha que $x \equiv y \pmod{m}$, ou seja, $x - y$ é divisível por m. Então $-(x - y) = y - x$ também é divisível por m, ou seja, $y \equiv x \pmod{m}$. Assim, a relação é simétrica.

(iii) Suponha agora que $x \equiv y \pmod{m}$ e $y \equiv z \pmod{m}$, portanto $x - y$ e $y - z$ são ambos divisíveis por m. Então, a soma

$$(x - y) + (y - z) = x - z$$

é também divisível por m, logo, $x \equiv z \pmod{m}$. Assim, a relação é transitiva.

Consequentemente, a relação de congruência módulo m sobre **Z** é de equivalência.

2.15 Seja A um conjunto de inteiros não nulos e seja $\approx$ a relação sobre $A \times A$ definida por

$$(a, b) \approx (c, d) \text{ se, e somente se, } ad = bc$$

Demonstre que $\approx$ é uma relação de equivalência.

Devemos mostrar que $\approx$ é reflexiva, simétrica e transitiva.

(i) *Reflexividade*: Temos $(a, b) \approx (a, b)$, uma vez que $ab = ba$. Logo, $\approx$ é reflexiva.

(ii) *Simetria*: Suponha que $(a, b) \approx (c, d)$. Então, $ad = bc$. Consequentemente, $cb = da$ e, assim, $(c, d) \approx (a, b)$. Logo, $\approx$ é simétrica.

(iii) *Transitividade*: Suponha que $(a, b) \approx (c, d)$ e $(c, d) \approx (e, f)$. Então, $ad = bc$ e $cf = de$. Multiplicando termos correspondentes das equações, temos $(ad)(cf) = (bc)(de)$. Cancelando $c \neq 0$ e $d \neq 0$ em ambos os lados da equação, temos $af = be$ e, portanto, $(a, b) \approx (e, f)$. Assim, $\approx$ é transitiva. Consequentemente, $\approx$ é uma relação de equivalência.

2.16 Seja R a seguinte relação de equivalência sobre o conjunto $A = \{1, 2, 3, 4, 5, 6\}$:

$R = \{(1, 1), (1, 5), (2, 2), (2, 3), (2, 6), (3, 2), (3, 3), (3, 6), (4, 4), (5, 1), (5, 5), (6, 2), (6, 3), (6, 6)\}$

Determine a partição de A induzida por R, ou seja, encontre as classes de equivalência de R.

Os elementos que se relacionam com 1 são 1 e 5 e, portanto,

$$[1] = \{1, 5\}$$

Escolhemos um elemento que não pertence a [1], digamos, 2. Os elementos relacionados a 2 são 2, 3 e 6 e, portanto,

$$[2] = \{2, 3, 6\}$$

O único elemento que não pertence a [1] ou [2] é 4. O único elemento que se relaciona com 4 é 4. Logo,

$$[4] = \{4\}$$

Consequentemente, a partição de A induzida por R é:

$$\{\{1, 5\}, \{2, 3, 6\}, \{4\}\}$$

2.17 Demonstre o Teorema 2.6: Seja R uma relação de equivalência em um conjunto A. Então o conjunto quociente A/R é uma partição de A. Especificamente,

(i) $a \in [a]$ para todo $a \in A$.

(ii) $[a] = [b]$ se, e somente se, $(a, b) \in R$.

(iii) Se $[a] \neq [b]$, então $[a]$ e $[b]$ são disjuntos.

(a) *Prova de (i)*: Como R é reflexiva, $(a, a) \in R$ para todo $a \in A$ e, portanto, $a \in [a]$.

(b) *Prova de (ii)*: Suponha que $(a, b) \in R$. Queremos demonstrar que $[a] = [b]$. Seja $x \in [b]$, então $(b, x) \in R$. Mas, por hipótese, $(a, b) \in R$ e, assim, por transitividade, $(a, x) \in R$. Consequentemente, $x \in [a]$. Então, $[b] \subseteq [a]$. Para provar que $[a] \subseteq [b]$, observamos que $(a, b) \in R$ implica, por simetria, que $(b, a) \in R$. Então, por argumento semelhante, obtemos $[a] \subseteq [b]$. Consequentemente, $[a] = [b]$.

Por outro lado, se $[a] = [b]$, então, por (i), $b \in [b] = [a]$; logo, $(a, b) \in R$.

(c) *Prova de* (iii): Demonstramos a afirmação contrapositiva equivalente:

$$\text{Se } [a] \cap [b] \neq \emptyset \quad \text{então} \quad [a] = [b]$$

Se $[a] \cap [b] \neq \emptyset$, então existe um elemento $x \in A$ com $x \in [a] \cap [b]$. Logo, $(a, x) \in R$ e $(b, x) \in R$. Por simetria, $(x, b) \in R$ e, por transitividade, $(a, b) \in R$. Portanto, por (ii), $[a] = [b]$.

Ordem parcial

2.18 Seja $\mathcal{C}$ uma coleção qualquer de conjuntos. A relação de inclusão conjuntista $\subseteq$ é uma ordem parcial em $\mathcal{C}$?

Sim, uma vez que a inclusão conjuntista é reflexiva, antissimétrica e transitiva. Isto é, para quaisquer conjuntos A, B, C, em $\mathcal{C}$ temos: (i) $A \subseteq A$, (ii) se $A \subseteq B$ e $B \subseteq A$, então $A = B$, (iii) se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

2.19 Considere o conjunto **Z** dos inteiros. Defina aRb por $b = a^r$ para algum inteiro positivo r. Mostre que R é uma ordem parcial em **Z**, ou seja, prove que R é: (a) reflexiva; (b) antissimétrica; (c) transitiva.

(a) R é reflexiva, pois $a = a^1$.

(b) Suponha que aRb e bRa, ou seja, $b = a^r$ e $a = b^s$. Logo, $a = (a^r)^s = a^{rs}$. Há três possibilidades: (i) $rs = 1$, (ii) $a = 1$, e (iii) $a = -1$. Se $rs = 1$, então $r = 1$ e $s = 1$ e, assim, $a = b$. Se $a = 1$, então $b = 1^r = 1 = a$ e, analogamente, se $b = 1$, então $a = 1$. Por último, se $a = -1$, então $b = -1$ (uma vez que $b \neq 1$) e $a = b$. Em todos os casos $a = b$. Portanto, R é antissimétrica.

(c) Suponha que aRb e bRc, ou seja, $b = a^r$ e $c = b^s$. Então $c = (a^r)^s = a^{rs}$ e, portanto, aRc. Logo, R é transitiva.

Consequentemente, R é uma ordem parcial sobre **Z**.

Problemas Complementares

Relações

2.20 Sejam $S = \{a, b, c\}$, $T = \{b, c, d\}$ e $W = \{a, d\}$. Encontre $S \times T \times W$.

2.21 Determine x e y, onde: (a) $(x + 2, 4) = (5, 2x + y)$; (b) $(y - 2, 2x + 1) = (x - 1, y + 2)$.

2.22 Prove: (a) $A \times (B \cap C) = (A \times B) \cap (A \times C)$; (b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

2.23 Considere a relação $R = \{(1, 3), (1, 4), (3, 2), (3, 3), (3, 4)\}$ sobre $A = \{1, 2, 3, 4\}$.

(a) Encontre a matriz M_R de R.

(b) Encontre o domínio e a imagem de R.

(c) Encontre R^{-1}.

(d) Esboce o grafo orientado de R.

(e) Determine a relação de composição $R \circ R$.

(f) Encontre $R \circ R^{-1}$ e $R^{-1} \circ R$.

2.24 Sejam $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$ e $C = \{x, y, z\}$. Considere as relações R de A em B e S de B em C como se segue

$$R = \{(1, b), (3, a), (3, b), (4, c)\} \quad \text{e} \quad S = \{(a, y), (c, x), (a, z)\}$$

(a) Esboce os diagramas de R e S.

(b) Encontre as matrizes de cada relação R, S e $R \circ S$ (composição).

(c) Escreva R^{-1} e a composição $R \circ S$ como conjuntos de pares ordenados.

2.25 Sejam R e S as seguintes relações sobre $B = \{a, b, c, d\}$:

$$R = \{(a, a), (a, c), (c, b), (c, d), (d, b)\} \text{ e } S = \{(b, a), (c, c), (c, d), (d, a)\}$$

Determine as seguintes relações de composição: (a) $R \circ S$; (b) $S \circ R$; (c) $R \circ R$; (d) $S \circ S$.

2.26 Seja R a relação sobre **N** definida por $x + 3y = 12$, ou seja, $R = \{(x, y) \mid x + 3y = 12\}$.

(a) Escreva R como um conjunto de pares ordenados. (c) Encontre R^{-1}.

(b) Determine o domínio e a imagem de R. (d) Encontre a relação de composição $R \circ R$.

Propriedades de relações

2.27 Cada um dos itens a seguir define uma relação sobre os inteiros positivos **N**.

(1) "x é maior que y."

(2) "xy é o quadrado de um inteiro."

(3) $x + y = 10$.

(4) $x + 4y = 10$.

Determine quais das relações são: (a) reflexivas, (b) simétricas; (c) antissimétricas, (d) transitivas.

2.28 Sejam R e S relações sobre um conjunto A. Assumindo que A tem pelo menos três elementos, estabeleça se cada uma das afirmações a seguir é verdadeira ou falsa. Se for falsa, dê um contraexemplo sobre o conjunto $A = \{1, 2, 3\}$.

(a) Se R e S são simétricas, então $R \cap S$ é simétrica.

(b) Se R e S são simétricas, então $R \cup S$ é simétrica.

(c) Se R e S são reflexivas, então $R \cap S$ é reflexiva.

(d) Se R e S são reflexivas, então $R \cup S$ é reflexiva.

(e) Se R e S são transitivas, então $R \cup S$ é transitiva.

(f) Se R e S são antissimétricas, então $R \cup S$ é antissimétrica.

(g) Se R é antissimétrica, então R^{-1} é antissimétrica.

(h) Se R é reflexiva, então $R \cap R^{-1}$ não é vazia.

(i) Se R é simétrica, então $R \cap R^{-1}$ não é vazia.

2.29 Suponha que R e S são relações sobre um conjunto A e que R é antissimétrica. Prove que $R \cap S$ é antissimétrica.

Relações de equivalência

2.30 Prove que, se R é uma relação de equivalência sobre um conjunto A, então R^{-1} também é uma relação de equivalência sobre A.

2.31 Seja $S = \{1, 2, 3, \ldots, 18, 19\}$. Seja R a relação sobre S definida por "xy é um quadrado". (a) Prove que R é uma relação de equivalência. (b) Encontre a classe de equivalência $[1]$. (c) Liste todas as classes de equivalência com mais de um elemento.

2.32 Seja $S = \{1, 2, 3, \ldots, 14, 15\}$. Seja R a relação de equivalência sobre S definida por $x \equiv y \ (mod\ 5)$, isto é, $x - y$ é divisível por 5. Determine a partição de S induzida por R, ou seja, o conjunto quociente S/R.

2.33 Sejam $S = \{1, 2, 3, \ldots, 9\}$ e $\sim$ a relação sobre $A \times A$ definida por

$$(a, b) \sim (c, d) \quad \text{se, e somente se,} \quad a + d = b + c$$

(a) Prove que $\sim$ é uma relação de equivalência.

(b) Encontre $[(2, 5)]$, ou seja, a classe de equivalência de $(2, 5)$.

Respostas dos Problemas Complementares

2.20 $\{(a, b, a), (a, b, d), (a, c, a), (a, c, d),$
$(a, d, a), (a, d, d), (b, b, a), (b, b, d),$
$(b, c, a), (b, c, d), (b, d, a), (b, d, d),$
$(c, b, a), (c, b, d), (c, c, a), (c, c, d),$
$(c, d, a), (c, d, d)\}$

2.21 (a) $x = 3, y = -2$; (b) $x = 2, y = 3$.

2.23 (a) $M_R = [0, 0, 1, 1, 0, 0, 0, 0,$
$0, 1, 1, 1, 0, 0, 0, 0]$,

(b) Domínio $= \{1, 3\}$, Imagem $= \{2, 3, 4\}$;

(c) $R^{-1} = \{(3, 1), (4, 1), (2, 3), (3, 3), (4, 3)\}$;

(d) Ver Fig. 2-8(a);

(e) $RoR = \{(1, 2), (1, 3), (1, 4), (3, 2),$
$(3, 3), (3, 4)\}$

2.24 (a) Ver Fig. 2-8(b);

(b) $R = [0, 1, 0; 0, 0, 0; 1, 1, 0; 0, 0, 1]$,
$S = [0, 1, 1, 0, 0, 0; 1, 0, 0]$,
$RoS = [0, 0, 0; 0, 0, 0; 0, 1, 1; 1, 0, 0]$;

(c) $\{(b, 1), (a, 3), (b, 3), (c, 4)\}$, $\{(3, y),$
$(3, z), (4, x)\}$.

2.25 (a) $R \circ S = \{(a, c), (a, d), (c, a), (d, a)\}$

(b) $S \circ R = \{(b, a), (b, c), (c, b), (c, d), (d, a), (d, c)\}$

(c) $R \circ R = \{(a, a), (a, b), (a, c), (a, d), (c, b)\}$

(d) $S \circ S = \{(c, c), (c, a), (c, d)\}$

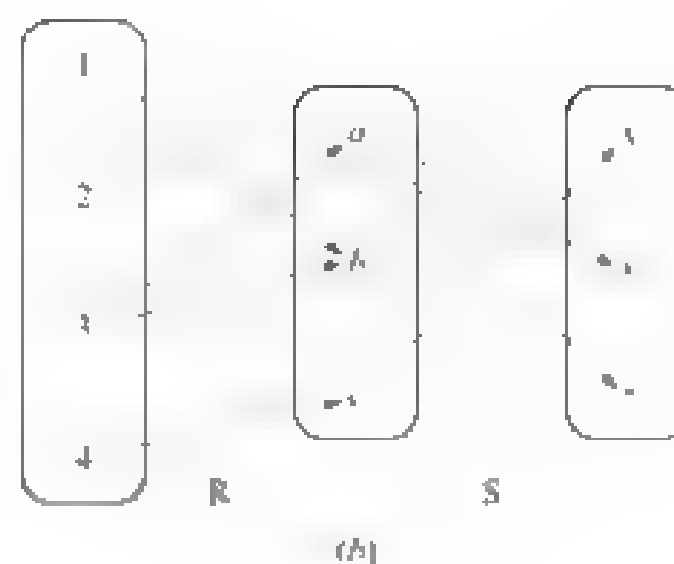
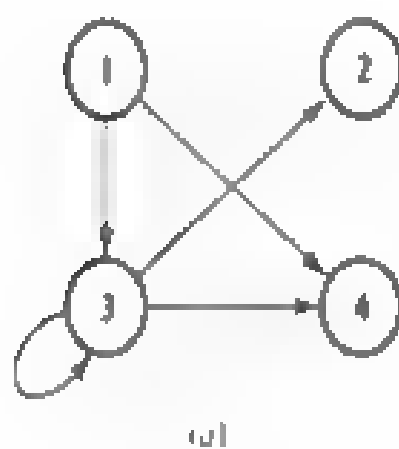



Figura 2-8

2.26 (a) $\{(9, 1), (6, 2), (3, 3)\}$, (b) (i) $\{9, 6, 3\}$, (ii) $\{1, 2, 3\}$, (iii) $\{(1, 9), (2, 6), (3, 3)\}$, (c) $\{(3, 3)\}$

2.27 (a) Nenhuma; (b) (2) e (3); (c) (1) e (4); (d) todas, exceto (3).

2.28 Todas são verdadeiras, exceto: (e) $R = \{(1, 2)\}$, $S = \{(2, 3)\}$; (f) $R = \{(1, 2)\}$, $S = \{(2, 1)\}$

2.31 (b) $\{1, 4, 9, 16\}$; (c) $\{1, 4, 9, 16\}$, $\{2, 8, 18\}$, $\{3, 12\}$.

2.32 $[\{1, 6, 11\}, \{2, 7, 12\}, \{3, 8, 133\}, \{4, 9, 14\}, \{5, 10, 15\}]$

2.33 (b) $\{(1, 4), (2, 5), (3, 6), (4, 7), (5, 8), (6, 9)\}$

Funções e Algoritmos

3.1 INTRODUÇÃO

Um dos conceitos mais importantes em matemática é o de função. Os termos "mapa", "mapeamento", "transformação" e muitos outros significam a mesma coisa, a escolha sobre qual terminologia empregar em uma dada situação geralmente é determinada pela tradição e pela formação matemática de quem usa o termo.

O conceito de algoritmo está relacionado com a noção de função. A notação para a apresentação de um algoritmo e uma discussão sobre sua complexidade também são abordadas neste capítulo.

3.2 FUNÇÕES

Suponha que a cada elemento de um conjunto A assinalamos um único elemento de um conjunto B; a coleção de tais correspondências é chamada de *função* de A em B. O conjunto A é denominado *domínio* da função e o conjunto B é chamado de *conjunto alvo* ou *codomínio*.

Funções são comumente denotadas por símbolos. Por exemplo, seja f uma função de A em B. Então escrevemos

$$f: A \to B$$

que se lê "f é uma função de A em B", ou "f leva (ou mapeia) A em B". Se $a \in A$, então $f(a)$ (lê-se, "f de a") denota o único elemento de B que f associa a a; ele é chamado de *imagem* de a sob f, ou o *valor* de f em a. O conjunto de todas as imagens é conhecido como a *imagem* de f. A imagem de $f: A \to B$ é denotada por $\text{Im}(f)$ ou $f(A)$.

Frequentemente, uma função pode ser expressa por meio de uma fórmula matemática. Por exemplo, considere a função que associa cada número real ao seu quadrado. Podemos descrever essa função como

$$f(x) = x^2 \quad \text{ou} \quad x \mapsto x^2 \quad \text{ou} \quad y = x^2$$

Na primeira notação, x é chamada de *variável* e a letra f denota a função. Na segunda notação, a flecha truncada $\mapsto$ se lê "leva em". Na última notação, x é conhecida como a *variável independente* e y é chamada de *variável dependente*, uma vez que o valor de y depende do valor de x.

Observação: Sempre que uma função é dada por uma fórmula em termos de uma variável x, assumimos, a menos que seja estabelecido o contrário, que o domínio da função é $\mathbf{R}$ (ou o maior subconjunto de $\mathbf{R}$ para o qual a fórmula tem significado) e o codomínio é $\mathbf{R}$.†

† N. de T. Vale observar que a noção de "maior subconjunto de $\mathbf{R}$" é meramente intuitiva, pois os autores não estabelecem critérios para determinar quando um conjunto infinito é maior do que outro conjunto infinito. A rigor, neste contexto, tal noção carece de sentido.

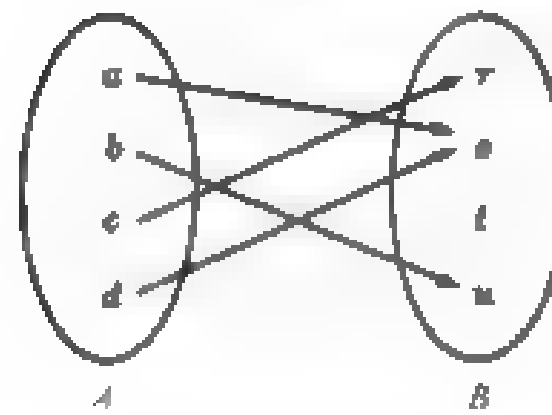



Figura 3-1

Exemplo 3.1

(a) Considere a função $f(x) = x^3$, isto é, f assinala a cada número real o seu cubo. Então a imagem de 2 é 8, e assim podemos escrever $f(2) = 8$.

(b) A Fig. 3-1 define uma função f de $A = \{a, b, c, d\}$ em $B = \{r, s, t, u\}$ na maneira óbvia. Aqui

$$f(a) = s, \quad f(b) = u, \quad f(c) = r, \quad f(d) = s$$

A imagem de f é o conjunto de valores de imagens, $\{r, s, u\}$. Note que t não pertence à imagem de f porque t não é imagem de elemento algum sob f.

(c) Seja A um conjunto qualquer. A função de A em A que assinala a cada elemento de A ele mesmo é chamada de *função identidade* sobre A e é usualmente denotada por 1_A ou, simplesmente, 1. Em outras palavras, para cada $a \in A$,

$$1_A(a) = a.$$

(d) Suponha que S é um subconjunto de A, ou seja, que $S \subset A$. O *mapa de inclusão* ou *mergulho* de S em A, denotado por $i: S \hookrightarrow A$, é a função tal que, para cada $x \in S$,

$$i(x) = x$$

A *restrição* de qualquer função $f: A \to B$, denotada por $f|_S$, é a função de S em B tal que, para cada $x \in S$,

$$f|_S(x) = f(x)$$

Funções e relações

Há outro ponto de vista do qual as funções podem ser consideradas. Em primeiro lugar, toda função $f: A \to B$ dá origem a uma relação de A em B conhecida como o *gráfico de* f, definido por

$$\text{Graf de } f = \{(a, b) \mid a \in A, b = f(a)\}$$

Duas funções $f: A \to B$ e $g: A \to B$ são definidas como *iguais*, e se escreve $f = g$, se $f(a) = g(a)$ para todo $a \in A$; isto é, se elas tiverem o mesmo gráfico. Consequentemente, não distinguimos entre uma função e seu gráfico. Agora, tal relação tem a propriedade de que cada a em A pertence a um único par ordenado (a, b) na relação. Por outro lado, qualquer relação f de A em B que tem essa propriedade dá origem a uma função $f: A \to B$, onde $f(a) = b$ para cada (a, b) em f. Logo, pode-se definir equivalentemente uma função como se segue:

Definição: Uma função $f: A \to B$ é uma relação de A em B (ou seja, um subconjunto de $A \times B$) tal que cada $a \in A$ pertence a um único par ordenado (a, b) em f.

A despeito de não diferenciarmos uma função de seu gráfico, ainda usamos a terminologia "gráfico de f" quando nos referimos a f como um conjunto de pares ordenados. Além disso, como o gráfico de f é uma relação, podemos esboçar seu desenho como foi feito para as relações em geral, e essa representação pictórica é ela mesma, às vezes, referida como gráfico de f. Também, a condição definidora de uma função, de que cada $a \in A$ pertence a um único par ordenado (a, b) em f, é equivalente à condição geométrica de cada reta vertical intersectando o gráfico em exatamente um ponto.

Exemplo 3.2

(a) Seja $f: A \to B$ a função definida no Exemplo 3.1(b). Então o gráfico de f é como se segue.

$$\{(a, s), (b, u), (c, r), (d, s)\}$$

(b) Considere as três relações a seguir sobre o conjunto $A = \{1, 2, 3\}$:

$$f = \{(1, 3), (2, 3), (3, 1)\} \qquad g = \{(1, 2), (3, 1)\} \qquad h = \{(1, 3), (2, 1), (1, 2), (3, 1)\}$$

f é uma função de A em A, uma vez que cada elemento de A aparece como a primeira coordenada em exatamente um par ordenado de f; aqui $f(1) = 3$, $f(2) = 3$ e $f(3) = 1$. g não é uma função de A em A, já que $2 \in A$ não é a primeira coordenada de qualquer par em g e, assim, g não assinala qualquer imagem a 2. Também h não é uma função de A em A, pois $1 \in A$ aparece como a primeira coordenada de dois pares ordenados distintos em h, $(1, 3)$ e $(1, 2)$. Se h fosse uma função, ele não assinalaria 3 e 2 ao elemento $1 \in A$.

(c) Por uma *função polinomial real*, queremos dizer uma função $f: \mathbf{R} \to \mathbf{R}$ da forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

onde os a_i são números reais. Como $\mathbf{R}$ é um conjunto infinito, seria impossível plotar cada ponto do gráfico. No entanto, o gráfico de tal função pode ser aproximado, primeiramente plotando alguns de seus pontos e então desenhando uma curva suave através desses pontos. Os pontos são geralmente obtidos a partir de uma tabela na qual vários valores são designados a x e os correspondentes valores de $f(x)$ são computados. A Fig. 3-2 ilustra essa técnica usando a função $f(x) = x^2 - 2x - 3$.

x	$f(x)$
−2	5
−1	0
0	−3
1	−4
2	−3
3	0
4	5

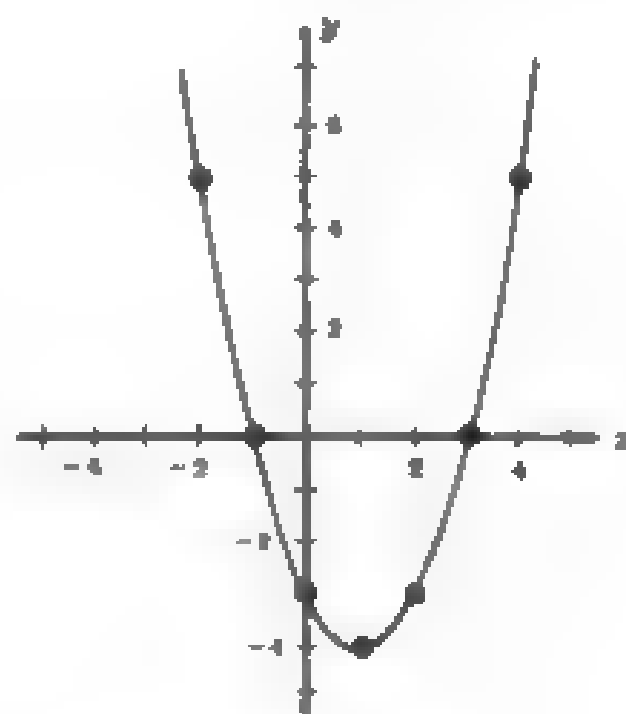



Gráfico de $f(x) = x^2 - 2x - 3$

Figura 3-2

Função composição

Considere as funções $f: A \to B$ e $g: B \to C$, isto é, tais que o codomínio de f é o domínio de g. Então podemos definir uma nova função de A em C, chamada de *composição* de f e g e denotada por $g \circ f$, como se segue:

$$(g \circ f)(a) \equiv g(f(a))$$

Ou seja, encontramos a imagem de a sob f e então determinamos a imagem de $f(a)$ sob g. Essa definição não é realmente nova. Se percebermos f e g como relações, então essa função é a mesma da composição de f e g enquan-

to relações (ver Seção 2.5), exceto que aqui usamos a notação funcional $g \circ f$ para a composição de f com g em vez da notação $f \circ g$ que era empregada para as relações.

Considere uma função qualquer $f: A \rightarrow B$. Então

$$f \circ 1_A = f \quad \text{e} \quad 1_B \circ f = f$$

onde 1_A e 1_B são as funções identidade sobre A e B, respectivamente.

3.3 FUNÇÕES INJETORAS, SOBREJETORAS E INVERSÍVEIS

Uma função $f: A \rightarrow B$ é dita *injetora* (ou *um para um*) se elementos diferentes do domínio A têm imagens distintas. Outra maneira de dizer a mesma coisa é que f é *injetora* se $f(a) = f(a')$ implica $a = a'$.

Uma função $f: A \rightarrow B$ é chamada de *sobrejetora* se cada elemento de B é a imagem de algum elemento de A. Em outras palavras, uma função $f: A \rightarrow B$ é sobrejetora se a imagem de f é o domínio inteiro, isto é, se $f(A) = B$. Neste caso dizemos que f é uma função de A sobre B ou que f mapeia A em B.

Uma função $f: A \rightarrow B$ é *inversível* se a sua relação inversa f^{-1} é uma função de B em A. Em geral, a relação inversa f^{-1} pode não ser uma função. O teorema a seguir fornece critérios simples que nos dizem quando é.

Teorema 3.1: Uma função $f: A \rightarrow B$ é inversível se, e somente se, f é injetora e sobrejetora.

Se $f: A \rightarrow B$ é injetora e sobrejetora, então f é dita uma *correspondência de um para um* (ou uma *bijeção*) entre A e B. Essa terminologia vem do fato de que cada elemento de A corresponde a um único elemento de B e vice-versa.

Alguns textos usam os termos *injetiva* para uma função injetora, *sobrejetiva* para uma função sobrejetora, e *bijetiva* (ou *bijetora*) para uma correspondência de um para um.

Exemplo 3.3 Considere as funções $f_1: A \rightarrow B$, $f_2: B \rightarrow C$, $f_3: C \rightarrow D$ e $f_4: D \rightarrow E$ definidas pelo diagrama da Fig. 3-3. Agora, f_1 é injetora, uma vez que nenhum elemento de B é a imagem de mais de um elemento de A. Analogamente, f_2 é injetora. Contudo, nem f_3 nem f_4 é injetora, pois $f_3(r) = f_3(u)$ e $f_4(v) = f_4(w)$.

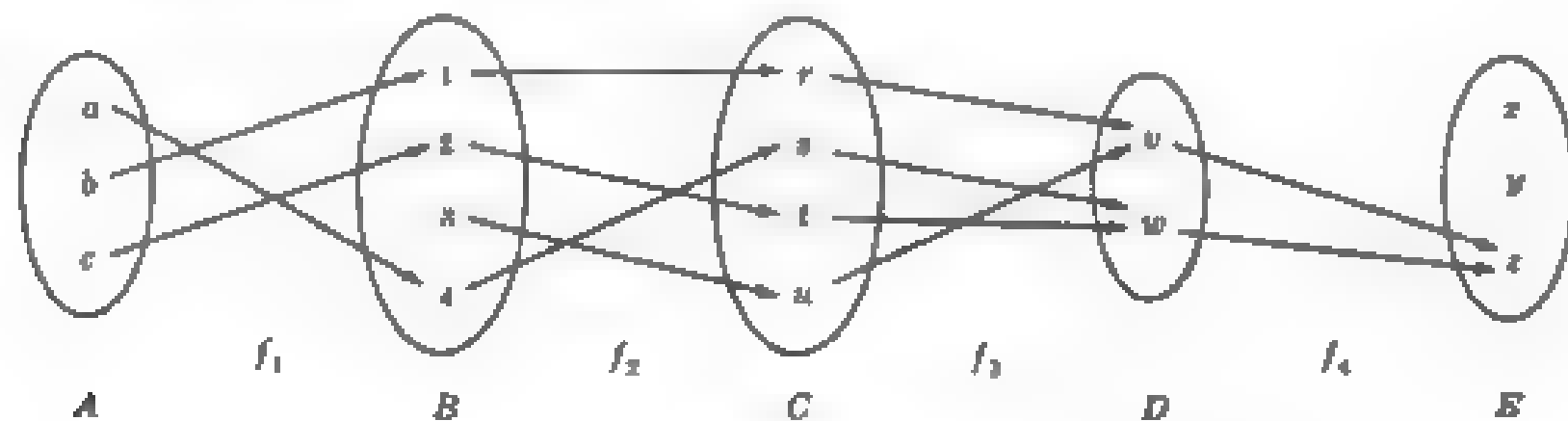



Figura 3-3

Quanto à sobrejetividade, f_2 e f_3 são ambas sobrejetoras, uma vez que cada elemento de C é a imagem sob f_2 de algum elemento de B, e cada elemento de D é a imagem sob f_3 de algum elemento de C, $f_2(B) = C$ e $f_3(C) = D$. Por outro lado, f_1 não é sobrejetora, pois $3 \in B$ não é imagem sob f_1 de qualquer elemento de A. E f_4 não é sobrejetora, pois $x \in E$ não é a imagem sob f_4 de qualquer elemento de D.

Assim, f_1 é injetora, mas não sobrejetora, f_3 é sobrejetora, mas não injetora, e f_4 não é injetora nem sobrejetora. No entanto, f_2 é injetora e sobrejetora, ou seja, é uma bijeção entre B e C. Logo, f_2 é inversível e f_2^{-1} é uma função de C em B.

Caracterização geométrica de funções injetoras e sobrejetoras

Considere agora funções da forma $f: \mathbf{R} \rightarrow \mathbf{R}$. Como os gráficos de tais funções podem ser plotados no plano cartesiano $\mathbf{R}^2$, e as funções podem ser identificadas pelos seus gráficos, podemos pensar se os conceitos de injetividade e sobrejetividade têm algum significado geométrico. A resposta é positiva. Especificamente:

(1) $f: \mathbf{R} \to \mathbf{R}$ é injetora se cada reta horizontal intersecta o gráfico de f em, no máximo, um ponto.

(2) $f: \mathbf{R} \to \mathbf{R}$ é uma função sobrejetora se cada reta horizontal intersecta o gráfico de f em um ou mais pontos.

Consequentemente, se f é injetora e sobrejetora, isto é, inversível, então cada reta horizontal intersecta o gráfico de f em exatamente um ponto.

Exemplo 3.4 Considere as quatro funções a seguir de **R** em **R**

$$f_1(x) = x^2, \qquad f_2(x) = 2^x, \qquad f_3(x) = x^3 - 2x^2 - 5x + 6, \qquad f_4(x) = x^3$$

Os gráficos dessas funções aparecem na Fig. 3-4. Observe que há retas horizontais que intersectam o gráfico de f_1 duas vezes e existem retas horizontais que não intersectam o gráfico de f_1, logo, f_1 não é injetora nem sobrejetora. Analogamente, f_2 é injetora, mas não sobrejetora, f_3 é sobrejetora, mas não injetora, e f_4 é injetora e sobrejetora. A inversa de f_4 é a função raiz cúbica, isto é, $f_4^{-1}(x) = \sqrt[3]{x}$.

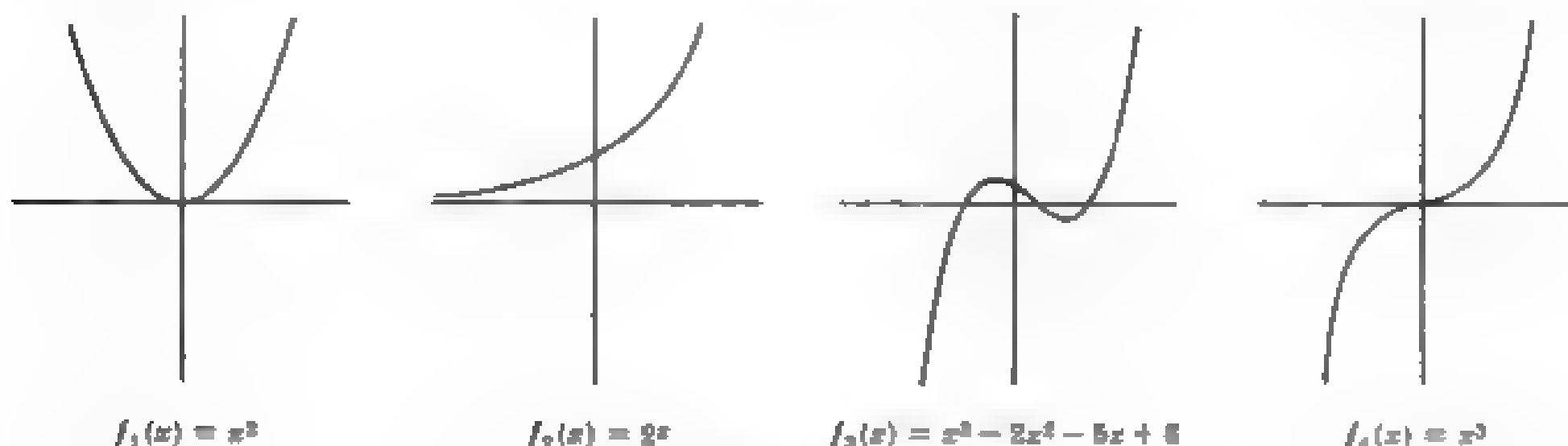



Figura 3-4

Permutações

Uma função inversível (bijetora) $\sigma: X \to X$ é chamada de *permutação* sobre X. A composição e a inversa de permutações sobre X, bem como a função identidade sobre X, são também permutações sobre X.

Suponha que $X = \{1, 2, \ldots, n\}$. Então uma permutação σ sobre X é frequentemente denotada por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ j_1 & j_2 & j_3 & \ldots & j_n \end{pmatrix}$$

onde $j_i = \sigma(i)$. O conjunto de todas essas permutações é denotado por S_n, e existem $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$ permutações. Por exemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{pmatrix} \quad \text{e} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 2 & 5 \end{pmatrix}$$

são permutações em S_6 e há $6! = 720$ permutações. Às vezes, escrevemos apenas a segunda linha da permutação, ou seja, denotamos as permutações acima por $\sigma = 462513$ e $\tau = 643125$.

3.4 FUNÇÕES MATEMÁTICAS, EXPONENCIAL E FUNÇÕES LOGARÍTMICAS

Esta seção apresenta várias funções matemáticas que surgem frequentemente na análise de algoritmos e na ciência da computação em geral, bem como as notações. Também discutimos as funções exponencial e logarítmica, e as relações entre elas.

Funções piso e teto

Seja x um número real qualquer. Então x está entre dois inteiros chamados de piso e teto de x. Especificamente,

> $\lfloor x \rfloor$, chamado de *piso* de x, denota o maior inteiro que não excede x.
> $\lceil x \rceil$, chamado de *teto* de x, denota o menor inteiro que não é menor do que x.

Se x é um inteiro, então $\lfloor x \rfloor = \lceil x \rceil$; caso contrário, $\lfloor x \rfloor + 1 = \lceil x \rceil$. Por exemplo,

$$\lfloor 3,14 \rfloor = 3, \quad \lfloor \sqrt{5} \rfloor = 2, \quad \lfloor -8,5 \rfloor = -9, \quad \lfloor 7 \rfloor = 7, \quad \lfloor -4 \rfloor = -4,$$

$$\lceil 3,14 \rceil = 4, \quad \lceil \sqrt{5} \rceil = 3, \quad \lceil -8,5 \rceil = -8, \quad \lceil 7 \rceil = 7, \quad \lceil -4 \rceil = -4$$

Funções inteiro e valor absoluto

Seja x um número real qualquer. O *valor inteiro* de x, escrito INT(x), converte x em um inteiro, deletando (truncando) a parte fracionária do número. Assim,

$$\text{INT}(3,14) = 3, \quad \text{INT}(\sqrt{5}) = 2, \quad \text{INT}(-8,5) = -8, \quad \text{INT}(7) = 7$$

Observe que $\text{INT}(x) = \lfloor x \rfloor$ ou $\text{INT}(x) = \lceil x \rceil$, dependendo se x é positivo ou negativo.

O *valor absoluto* do número real x, escrito ABS(x) ou $|x|$, é definido como o maior entre x e $-x$. Logo, $\text{ABS}(0) = 0$ e, para $x \neq 0$, $\text{ABS}(x) = x$ ou $\text{ABS}(x) = -x$, dependendo se x é positivo ou negativo. Logo,

$$|-15| = 15, \quad |7| = 7, \quad |-3,33| = 3,33, \quad |4,44| = 4,44, \quad |-0,075| = 0,075$$

Observamos que $|x| = |-x|$ e, para $x \neq 0$, $|x|$ é positivo.

Função resto e aritmética modular

Sejam k um inteiro qualquer e M um inteiro positivo. Então

$$k \ (\text{mod } M)$$

(lê-se: k módulo M) denota o resto inteiro quando k é dividido por M. Mais exatamente k (mod M) é o único inteiro r tal que

$$k = Mq + r \quad \text{onde} \quad 0 \leq r < M$$

Quando k é positivo, simplesmente divida k por M para obter o resto r. Assim,

$$25 \ (\text{mod } 7) = 4, \quad 25 \ (\text{mod } 5) = 0, \quad 35 \ (\text{mod } 11) = 2, \quad 3 \ (\text{mod } 8) = 3$$

Se k é negativo, divida $|k|$ por M para obter um resto r', então k (mod M) $= M - r'$ quando $r' \neq 0$. Logo,

$$-26 \ (\text{mod } 7) = 7 - 5 = 2, \quad -371 \ (\text{mod } 8) = 8 - 3 = 5, \quad -39 \ (\text{mod } 3) = 0$$

O termo "mod" é também usado para a relação de congruência matemática, que é definida e denotada como se segue:

$$a \equiv b \ (\text{mod } M) \quad \text{se, e somente se,} \quad M \text{ divide } b - a$$

M é chamado de *módulo*, e $a \equiv b$ (mod M) se lê "a é congruente a b módulo M". Os seguintes aspectos da relação de congruência são frequentemente úteis:

$$0 \equiv M \ (\text{mod } M) \quad \text{e} \quad a \pm M \equiv a \ (\text{mod } M)$$

Aritmética módulo M se refere às operações aritméticas de adição, multiplicação e subtração onde o valor aritmético é substituído por seu valor equivalente no conjunto

$$\{0, 1, 2, \ldots, M-1\} \quad \text{ou no conjunto} \quad \{1, 2, 3, \ldots, M\}$$

Por exemplo, na aritmética módulo 12, às vezes conhecida como aritmética "do relógio",

$$6+9=3, \quad 7\times 5=11, \quad 1-5=8, \quad 2+10=0=12$$

(o uso de 0 ou M depende da aplicação.)

Funções exponenciais

Lembre as seguintes definições para expoentes inteiros (onde m é um inteiro positivo).

$$a^m = a\cdot a\cdots a\ (m \text{ ocorrências}), \qquad a^0 = 1, \qquad a^{-m} = \frac{1}{a^m}$$

Expoentes são estendidos para incluir todos os números racionais, definindo, para qualquer número racional m/n,

$$a^{m/n} = \sqrt[n]{a^m} = (\sqrt[n]{a})^m$$

Por exemplo,

$$2^4 = 16, \quad 2^{-4} = \frac{1}{2^4} = \frac{1}{16}, \quad 125^{2/3} = 5^2 = 25$$

De fato, expoentes são estendidos para incluir todos os números reais, definindo, para qualquer número real x,

$$a^x = \lim_{r\to x} a^r, \quad \text{onde } r \text{ é um número racional}$$

Consequentemente, a função exponencial $f(x) = a^x$ é definida para todos os números reais.

Funções logarítmicas

Logaritmos são relacionados com expoentes como se segue. Seja b um número positivo. O logaritmo de qualquer número positivo x na base b, escrito como

$$\log_b x$$

representa o expoente ao qual b deve ser elevado para obter x. Ou seja,

$$y = \log_b x \quad \text{e} \quad b^y = x$$

são afirmações equivalentes. Consequentemente,

$$\begin{array}{llllll} \log_2 8 = 3 & \text{pois} & 2^3 = 8; & \log_{10} 100 = 2 & \text{pois} & 10^2 = 100 \\ \log_2 64 = 6 & \text{pois} & 2^6 = 64; & \log_{10} 0{,}001 = -3 & \text{pois} & 10^{-3} = 0{,}001 \end{array}$$

Além disso, para qualquer base b, temos $b^0 = 1$ e $b^1 = b$; logo,

$$\log_b 1 = 0 \quad \text{e} \quad \log_b b = 1$$

O logaritmo de um número negativo e o logaritmo de 0 não são definidos.

Frequentemente, logaritmos são expressos usando valores aproximados. Por exemplo, utilizando tabelas ou calculadoras, obtem-se

$$\log_{10} 300 = 2{,}4771 \quad \text{e} \quad \log_e 40 = 3{,}6889$$

como respostas aproximadas. (Aqui $e = 2{,}718281\ldots$.)

Três classes de logaritmos são de especial interesse: logaritmos na base 10, conhecidos como *logaritmos comuns*; na base e, conhecidos como *logaritmos naturais*; e na base 2, conhecidos como *logaritmos binários*. Alguns textos denotam

$$\ln x \text{ para } \log_e x \qquad \text{e} \qquad \lg x \text{ ou } \log x \text{ para } \log_2 x$$

O termo x geralmente significa $\log_{10} x$; mas é também empregado para $\log_e x$ em textos matemáticos avançados e para $\log_2 x$ em textos de ciência da computação.

Frequentemente, exigimos apenas o piso ou o teto de um logaritmo binário. Isso pode ser obtido examinando-se as potências de 2. Por exemplo,

$$\lfloor \log_2 100 \rfloor = 6, \quad \text{pois} \quad 2^6 = 64 \quad \text{e} \quad 2^7 = 128$$
$$\lceil \log_2 1000 \rceil = 9, \quad \text{pois} \quad 2^9 = 512 \quad \text{e} \quad 2^{10} = 1024$$

e assim por diante.

Relação entre as funções exponencial e logarítmica

A relação básica entre as funções exponencial e logarítmica

$$f(x) = b^x \quad \text{e} \quad g(x) = \log_b x$$

é que elas são a inversa uma da outra; portanto, os gráficos dessas funções são relacionados geometricamente. Essa relação é ilustrada na Fig. 3-5, na qual os gráficos da função exponencial $f(x) = 2^x$, da função logarítmica $g(x) = \log_2 x$ e da função linear $h(x) = x$ aparecem nos mesmos eixos coordenados. Como $f(x) = 2^x$ e $g(x) = \log_2 x$ são funções inversas, elas são simétricas com relação à função linear $h(x) = x$ ou, em outras palavras, a reta $y = x$.

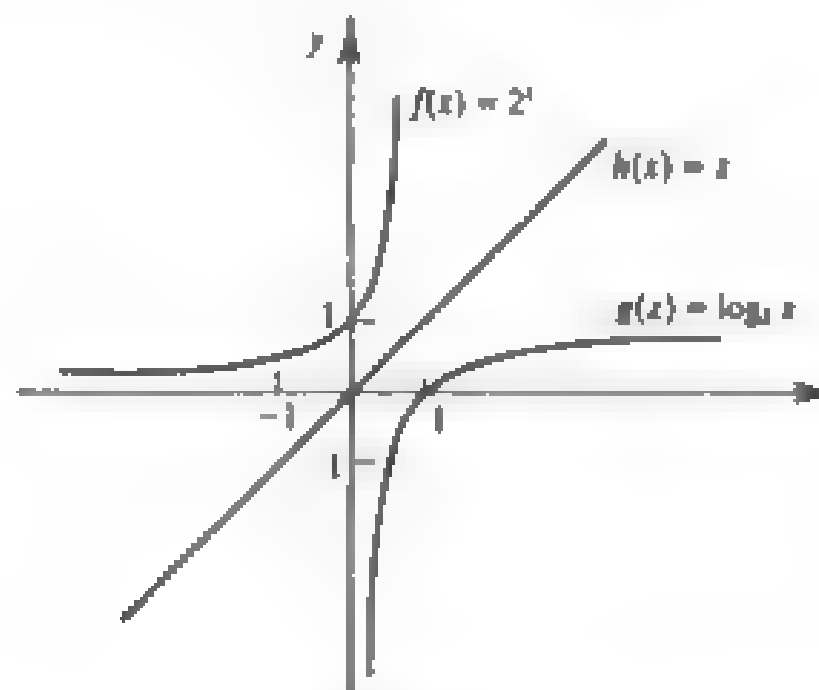



Figura 3-5

A Fig. 3-5 também indica outra propriedade importante das funções exponencial e logarítmica. Especificamente, para qualquer positivo c, temos

$$g(c) < h(c) < f(c), \qquad \text{isto é,} \qquad g(c) < c < f(c)$$

De fato, à medida que c cresce em valor, as distâncias verticais $h(c) - g(c)$ e $f(c) - g(c)$ aumentam. Além disso, a função logarítmica $g(x)$ cresce muito lentamente comparada com a função linear $h(x)$, e a exponencial $f(x)$ cresce muito rapidamente em comparação com $h(x)$.

3.5 SEQUÊNCIAS, CLASSES INDEXADAS DE CONJUNTOS

Sequências e classes indexadas de conjuntos são tipos especiais de funções com sua própria notação. Discutimos a notação de somatório aqui.

Sequências

Uma *sequência* é uma função do conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ de números inteiros positivos em um conjunto A. A notação a_n é usada para denotar a imagem do inteiro n. Assim, uma sequência é geralmente denotada por

$$a_1, a_2, a_3, \ldots \quad \text{ou} \quad \{a_n : n \in \mathbf{N}\} \quad \text{ou} \quad \text{simplesmente} \quad \{a_n\}$$

Às vezes o domínio de uma sequência é o conjunto $\{0, 1, 2, \ldots\}$ de inteiros não negativos, em vez de $\mathbf{N}$. Em tal caso, dizemos que n começa com 0 e não com 1.

Uma *sequência finita* sobre um conjunto A é uma função de $\{1, 2, \ldots, m\}$ em A e é usualmente denotada por

$$a_1, a_2, \ldots, a_m$$

Tal sequência finita é, às vezes, chamada de *lista* ou *m-upla*.

Exemplo 3.5

(a) Eis duas sequências conhecidas:

(i) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ que pode ser definida por $a_n = \frac{1}{n}$;

(ii) $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$ que pode ser definida por $b_n = 2^{-n}$

Note que a primeira sequência começa com $n = 1$ e a segunda inicia com $n = 0$.

(b) A importante sequência $1, -1, 1, -1, \ldots$ pode ser formalmente definida por

$$a_n = (-1)^{n+1} \text{ ou, equivalentemente, por } b_n = (-1)^n$$

onde a primeira sequência começa com $n = 1$ e a segunda inicia com $n = 0$.

(c) *Strings* Suponha que um conjunto A é finito, e A é visto como um conjunto de caracteres ou um alfabeto. Então uma sequência finita sobre A é chamada de *string* ou *palavra*, e é geralmente representada na forma $a_1a_2 \ldots a_m$, ou seja, sem parênteses. O número m de caracteres no string é conhecido como o seu *comprimento*. Percebe-se também o conjunto com zero caracteres como um string; ele é chamado de *string vazio* ou *string nulo*. Strings sobre um alfabeto A e certas operações sobre esses strings são discutidos detalhadamente no Capítulo 13.

Símbolo de somatório, somas

Introduzimos aqui o símbolo de somatório $\sum$ (a letra grega sigma). Considere uma sequência $a_1, a_2, a_3, \ldots$ Então definimos o que se segue:

$$\sum_{j=1}^{n} a_j = a_1 + a_2 + \cdots + a_n \qquad \text{e} \qquad \sum_{j=m}^{n} a_j = a_m + a_{m+1} + \cdots + a_n$$

A letra j na expressão acima é chamada de *índice*. Outras letras frequentemente empregadas como índices são i, k, s e t.

Exemplo 3.6

$$\sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

$$\sum_{j=2}^{5} j^2 = 2^2 + 3^2 + 4^2 + 5^2 = 4 + 9 + 16 + 25 = 54$$

$$\sum_{j=1}^{n} j = 1 + 2 + \cdots + n$$

A última soma aparece com muita frequência. Ela tem o valor $n(n+1)/2$. Ou seja:

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}, \quad \text{por exemplo,} \quad 1+2+\cdots+50=\frac{50(51)}{2}=1275$$

Classes indexadas de conjuntos

Sejam I um conjunto não vazio e S uma coleção de conjuntos. Uma *função indexadora* de I em S é uma função $f: I \to S$. Para qualquer $i \in I$, denotamos a imagem $f(i)$ por A_i. Assim, a função indexadora f é normalmente denotada por

$$\{A_i \mid i \in I\} \quad \text{ou} \quad \{A_i\}_{i \in I} \quad \text{ou} \quad \text{simplesmente } \{A_i\}$$

O conjunto I é chamado de *conjunto indexador*, e os elementos de I são chamados de *índices*. Se f é injetora e sobrejetora, dizemos que S é indexado por I.

Os conceitos de união e interseção são definidos para classes indexadas de conjuntos como se segue.

$$\cup_{i \in I} A_i = \{x \mid x \in A_i \text{ para algum } i \in I\} \text{ e } \cap_{i \in I} A_i = \{x \mid x \in A_i \text{ para todo } i \in I\}$$

No caso em que I é um conjunto finito, essa é exatamente a mesma definição anterior de união e interseção. Se I é $\mathbf{N}$, podemos denotar a união e a interseção, respectivamente, como se segue:

$$A_1 \cup A_2 \cup A_3 \cup \cdots \quad \text{e} \quad A_1 \cap A_2 \cap A_3 \cap \cdots$$

Exemplo 3.7 Seja I o conjunto $\mathbf{Z}$ dos inteiros. Para cada $n \in \mathbf{Z}$, assinalamos o seguinte intervalo infinito em $\mathbf{R}$.

$$A_n = \{x \mid x \le n\} = (-\infty, n]$$

Para qualquer número real a, existem inteiros n_1 e n_2 tais que $n_1 < a < n_2$, logo, $a \in A_{n_2}$, mas $a \notin A_{n_1}$. Assim,

$$a \in \cup_n A_n \quad \text{mas} \quad a \notin \cap_n A_n$$

Consequentemente,

$$\cup_n A_n = \mathbf{R} \quad \text{mas} \quad \cap_n A_n = \emptyset$$

3.6 FUNÇÕES RECURSIVAMENTE DEFINIDAS

Uma função é dita *recursivamente definida* se a definição da função se refere a ela mesma. Para que a definição da função não seja circular, ela deve ter as duas propriedades a seguir:

(1) Deve haver certos argumentos, chamados de *valores base*, para os quais a função não faça referência a si mesma.

(2) Cada vez que a função se refira a si mesma, o argumento da função deve ficar mais próximo a um valor base.

Uma função recursiva com essas duas propriedades é dita *bem definida*.

Os seguintes exemplos devem ajudar a esclarecer essas ideias.

Função fatorial

O produto dos inteiros positivos de 1 a n, inclusive, é chamado de "n fatorial" e geralmente é denotado por $n!$. Isto é,

$$n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$$

É também conveniente definir $0! = 1$, de modo que a função é definida para todos os inteiros não negativos. Assim:

$$0! = 1, \quad 1! = 1, \quad 2! = 2 \cdot 1 = 1, \quad 3! = 3 \cdot 2 \cdot 1 = 6, \quad 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24,$$

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120, \quad 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$$

E assim por diante. Observe que

$$5! = 5 \cdot 4! = 5 \cdot 24 = 120 \quad \text{e} \quad 6! = 6 \cdot 5! = 6 \cdot 120 = 720$$

Isso é verdadeiro para todo inteiro positivo; isto é,

$$n! = n \cdot (n-1)!$$

Consequentemente, a função fatorial pode também ser definida como se segue:

Definição 3.1 (função fatorial)

(a) Se $n = 0$, então $n! = 1$

(b) Se $n > 0$, então $n! = n \cdot (n-1)!$

Note que a definição acima de $n!$ é recursiva, uma vez que ela se refere a si mesma quando usa $(n-1)!$. Contudo:

(1) O valor de $n!$ é explicitamente dado quando $n = 0$ (assim, 0 é um valor base).

(2) O valor de $n!$ para n arbitrário é definido em termos de um valor menor de n que é mais próximo do valor base 0.

Consequentemente, a definição não é circular ou, em outras palavras, a função é bem definida.

Exemplo 3.8 A Fig. 3-6 mostra os nove passos para calcular $4!$, usando a definição recursiva. Especificamente:

Passo 1. Este define $4!$ em termos de $3!$, portanto, devemos adiar o cálculo de $4!$ até calcularmos 3. Esse adiamento é indicado, deslocando para direita o próximo passo.

Passo 2. Aqui $3!$ é definido em termos de $2!$, logo, devemos adiar o cálculo de $3!$ até calcularmos $2!$.

Passo 3. Este define $2!$ em termos de $1!$.

Passo 4. Este define $1!$ em termos de $0!$.

Passo 5. Este passo pode explicitamente calcular $0!$, pois 0 é o valor base da definição recursiva

Passos 6 a 9. Voltamos, usando $0!$ para encontrar $1!$, usando $1!$ para encontrar $2!$, usando $2!$ para encontrar $3!$ e finalmente usando $3!$ para encontrar $4!$. O retorno é indicado pelo deslocamento para a esquerda.

Observe que retornamos na ordem inversa dos cálculos originalmente adiados.

(1) $4! = 4 \cdot 3!$

(2) $3! = 3 \cdot 2!$

(3) $2! = 2 \cdot 1!$

(4) $1! = 1 \cdot 0!$

(5) $0! = 1$

(6) $1! = 1 \cdot 1 = 1$

(7) $2! = 2 \cdot 1 = 2$

(8) $3! = 3 \cdot 2 = 6$

(9) $4! = 4 \cdot 6 = 24$

Figura 3-6

Números de nível

Seja P um procedimento ou fórmula recursiva que é usada para calcular $f(X)$, onde f é uma função recursiva e X é a entrada. Associamos um *número de nível* para cada execução de P como se segue. A execução original de P é designada nível 1, e cada vez que P é executado por conta de uma chamada recursiva, seu nível é um a mais do que o nível da execução que fez a chamada recursiva. A *profundidade* da recursão no cálculo de $f(X)$ se refere ao número de nível máximo de P durante sua execução.

Considere, por exemplo, o cálculo de 4! no Exemplo 3.8, que utiliza a fórmula recursiva $n! = n(n-1)!$ O Passo 1 pertence ao nível 1, uma vez que é a primeira execução da fórmula. Assim.

Passo 2 pertence ao nível 2, Passo 3 pertence ao nível 3,..., Passo 5 pertence ao nível 5

Por outro lado, o Passo 6 pertence ao nível 4, uma vez que é o resultado de um retorno do nível 5. Em outras palavras, Passos 6 e 4 pertencem ao mesmo nível de execução. Analogamente,

Passo 7 pertence ao nível 3; Passo 8 pertence ao nível 2, Passo 9 pertence ao nível 1.

Consequentemente, para calcular 4!, a profundidade da recursão é 5.

Sequência de Fibonacci

A célebre sequência de Fibonacci (geralmente denotada por $F_0, F_1, F_2, \ldots$) é como se segue:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad 55, \quad \ldots$$

Ou seja, $F_0 = 0$ e $F_1 = 1$ e cada termo subsequente é a soma dos dois termos precedentes. Por exemplo, os próximos dois termos da sequência são

$$34 + 55 = 89 \text{ e } 55 + 89 = 144$$

Uma definição formal dessa função é a seguinte:

Definição 3.2 (sequência de Fibonacci):

(a) Se $n = 0$ ou $n = 1$, então $F_n = n$

(b) Se $n > 1$, então $F_n = F_{n-2} + F_{n-1}$.

Esse é outro exemplo de uma definição recursiva, pois a definição se refere a ela mesma quando usa F_{n-2} e F_{n-1}. No entanto:

(1) Os valores base são 0 e 1.

(2) O valor de F_n é definido em termos de valores menores de n que são mais próximos dos valores base.

Consequentemente, essa função é bem definida.

Função de Ackermann

A função de Ackermann é uma função com dois argumentos, sendo que a cada um deles pode ser assinalado qualquer inteiro não negativo, isto é, 0, 1, 2,.... Essa função é definida como:

Definição 3.3 (Função de Ackermann)

(a) Se $m = 0$, então $A(m, n) = n + 1$.

(b) Se $m \neq 0$, mas $n = 0$, então $A(m, n) = A(m - 1, 1)$.

(c) Se $m \neq 0$ e $n \neq 0$, então $A(m, n) = A(m - 1, A(m, n - 1))$.

Mais uma vez, temos uma definição recursiva, já que a definição se refere a ela mesma nos itens (*b*) e (*c*). Observe que $A(m, n)$ é explicitamente dado apenas quando $m = 0$. Os critérios base são os pares

$$(0, 0), \quad (0, 1), \quad (0, 2), \quad (0, 3), \quad \ldots, (0, n), \quad \ldots$$

Apesar de não ser óbvio a partir dessa definição, o valor de qualquer $A(m, n)$ pode eventualmente ser expresso em termos do valor da função sobre um ou mais pares base.

O valor de $A(1, 3)$ é calculado no Problema 3.21. Mesmo esse caso simples requer 15 passos. Em termos gerais, a função de Ackermann é muito complexa para calcular sobre qualquer exemplo que não seja trivial. Sua importância vem de seu emprego em lógica matemática. A função é exibida aqui, principalmente, para dar outro exemplo de uma função recursiva clássica e para mostrar que a parte de recursão de uma definição pode ser complicada.

3.7 CARDINALIDADE

Dois conjuntos A e B são ditos *equipotentes*, ou tendo o *mesmo número de elementos* ou a *mesma cardinalidade*, denotando-se por $A \simeq B$, se existe uma correspondência de um-para-um $f: A \to B$. Um conjunto A é *finito* se A é vazio ou se A tem a mesma cardinalidade do conjunto $\{1, 2, \ldots, n\}$ para algum inteiro positivo n. Um conjunto é *infinito* se não for finito.† Exemplos de conjuntos infinitos são o dos números naturais **N**, o dos inteiros **Z**, o dos racionais **Q** e o dos números reais **R**.

Introduzimos agora a ideia de "números cardinais". Consideramos números cardinais simplesmente como símbolos designados a conjuntos, de tal maneira que dois conjuntos são associados ao mesmo símbolo se, e somente se, eles têm a mesma cardinalidade. O número cardinal de um conjunto A é comumente denotado por $|A|$, $n(A)$ ou (A). Usamos $|A|$.

Os símbolos óbvios são usados para a cardinalidade de conjuntos finitos. Isto é, 0 é designado para o conjunto vazio $\emptyset$ e n é designado para o conjunto $\{1, 2, \ldots, n\}$. Assim, $|A| = n$ se, e somente se, A tem n elementos. Por exemplo,

$$|\{x, y, z\}| = 3 \quad \text{e} \quad |\{1, 3, 5, 7, 9\}| = 5$$

O número cardinal do conjunto infinito **N** dos inteiros positivos é $\aleph_0$ ("álef zero"). Esse símbolo foi introduzido por Cantor. Logo, $|A| = \aleph_0$ se, e somente se, A tem a mesma cardinalidade de **N**.

Exemplo 3.9 Seja $E = \{2, 4, 6, \ldots\}$ o conjunto dos inteiros positivos pares. A função $f: \mathbf{N} \to E$ definida por $f(n) = 2n$ é uma correspondência bijetora entre os inteiros positivos **N** e E. Assim, E tem a mesma cardinalidade de **N** e, portanto, podemos escrever

$$|E| = \aleph_0$$

Um conjunto com cardinalidade $\aleph_0$ é dito *enumerável* ou *infinitamente contável*. Um conjunto que seja finito ou enumerável é dito *contável*. É possível mostrar que o conjunto **Q** dos números racionais é contável. De fato, temos o seguinte teorema (provado no Problema 3.13) que usamos subsequentemente.

Teorema 3.2: Uma união contável de conjuntos contáveis é contável.
Ou seja, se $A_1, A_2, \ldots$ são conjuntos contáveis, então a união a seguir é contável.

$$A_1 \cup A_2 \cup A_3 \cup \ldots$$

Um exemplo importante de um conjunto infinito que é incontável, ou seja, não contável, é dado pelo seguinte teorema, o qual é demonstrado no Problema 3.14.

Teorema 3.3: O conjunto **I** de todos os números reais entre 0 e 1 não é contável.

Desigualdades e números cardinais

Deseja-se também comparar o tamanho de dois conjuntos. Isso é conseguido por meio de uma relação de desigualdade que é definida para números cardinais como se segue. Para quaisquer conjuntos A e B, definimos $|A| \leq |B|$ se existir uma função $f: A \to B$ que seja injetora. Também escrevemos

$$|A| < |B|, \text{ se } |A| \leq |B|, \text{ mas } |A| \neq |B|$$

† N. de T. Outra definição mais usual estabelece que um conjunto x é infinito se existir subconjunto próprio y de x tal que x e y sejam equipotentes. Já conjunto finito é aquele que não é infinito.

Por exemplo, $|\mathbf{N}| < |\mathbf{I}|$, onde $\mathbf{I} = \{x : 0 < x < 1\}$, uma vez que a função $f : \mathbf{N} \to \mathbf{I}$ definida por $f(n) = 1/n$ é injetora, mas $|\mathbf{N}| \neq |\mathbf{I}|$, pelo Teorema 3.3.

O Teorema de Cantor, que vem a seguir e é demonstrado no Problema 3.25, nos diz que os números cardinais não são cotados.

Teorema 3.4 (Cantor): Para qualquer conjunto A, temos $|A| < |\text{Potência}(A)|$ (onde Potência(A) é o conjunto potência de A, isto é, a coleção de todos os subconjuntos de A).

O próximo teorema nos diz que a relação de desigualdade para números cardinais é antissimétrica:

Teorema 3.5 (Schroeder-Bernstein): Suponha que A e B são conjuntos tais que

$$|A| \leq |B| \quad \text{e} \quad |B| \leq |A|$$

Então $|A| = |B|$.

Provamos uma formulação equivalente desse teorema no Problema 3.26.

3.8 ALGORITMOS E FUNÇÕES

Um algoritmo M é uma lista finita passo a passo de instruções bemdefinidas para resolver um problema em particular, por exemplo, a saída $f(X)$ para uma dada função f com entrada X. (Aqui X pode ser uma lista ou conjunto de valores.) Frequentemente, pode haver mais de uma maneira para obter $f(X)$, como ilustrado pelos exemplos a seguir. A escolha particular do algoritmo M para obter $f(X)$ pode depender da "eficiência" ou da "complexidade" do algoritmo; a questão da complexidade de um algoritmo M é formalmente discutida na próxima seção.

Exemplo 3.10 (Cálculo Polinomial) Suponha que, para um dado polinômio $f(x)$ e um valor $x = a$, queremos achar $f(a)$, como

$$f(x) = 2x^3 - 7x^2 + 4x - 15 \quad \text{e} \quad a = 5$$

Isso pode ser feito das duas maneiras a seguir.

(a) (***Método Direto***): Aqui substituímos $a = 5$ diretamente no polinômio para obter

$$f(5) = 2(125) - 7(25) + 4(5) - 7 = 250 - 175 + 20 - 15 = 80$$

Observe que há $3 + 2 + 1 = 6$ multiplicações e 3 adições. No caso geral, calcular diretamente um polinômio de grau n requer aproximadamente

$$n + (n-1) + \cdots + 1 = \frac{n(n+1)}{2} \text{ multiplicações e } n \text{ adições.}$$

(b) (***Método de Horner ou Divisão Sintética***): Aqui reescrevemos o polinômio sucessivamente, evidenciando x como se segue:

$$f(x) = (2x^2 - 7x + 4)x - 15 = ((2x - 7)x + 4)x - 15$$

Então

$$f(5) = ((3)5 + 4)5 - 15 = (19)5 - 15 = 95 - 15 = 80$$

Para aqueles familiarizados com a divisão sintética, a aritmética acima é equivalente à seguinte divisão sintética:

$$\begin{array}{r|rrrrrrr} 5 & 2 & - & 7 & + & 4 & - & 15 \\ & & & 10 & + & 15 & + & 95 \\ \hline & 2 & + & 3 & + & 19 & + & 80 \end{array}$$

Observe que aqui há 3 multiplicações e 3 adições. No caso geral, calcular um polinômio de grau n pelo método de Horner requer aproximadamente

$$n \text{ multiplicações e } n \text{ adições}$$

Claramente o método de Horner (*b*) é mais eficiente do que o direto (*a*).

Exemplo 3.11 (Máximo Divisor Comum) Sejam a e b inteiros positivos com, digamos, $b < a$; e suponha que queremos encontrar $d = \text{MDC}(a, b)$, o máximo divisor comum entre a e b. Isso pode ser feito de duas maneiras.

(a) (***Método Direto***): Aqui encontramos todos os divisores de a, por exemplo, testando todos os números de 2 a $a/2$, e todos os divisores de b. Então escolhemos o maior divisor comum. Por exemplo, suponha que $a = 258$ e $b = 60$. Os divisores de a e b são:

$a = 258$: divisores: 1, 2, 3, 6, 86, 129, 258
$b = 60$: divisores: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

Consequentemente, $d = \text{MDC}(258, 60) = 6$.

(b) (***Algoritmo Euclidiano***): Aqui dividimos a por b para obter um resto r_1. (Note que $r_1 < b$.) Em seguida, dividimos b pelo resto r_1 para obter um segundo resto r_2. (Note que $r_2 < r_1$.) Depois, dividimos r_1 por r_2 para obter um terceiro resto r_3. (Note que $r_3 < r_2$.) Continuamos dividindo r_k por r_{k+1} para obter um resto r_{k+2}. Como

$$a > b > r_1 > r_2 > r_3 \ldots \qquad (*)$$

eventualmente obtemos um resto $r_m = 0$. Então, $r_{m-1} = \text{MDC}(a, b)$. Por exemplo, suponha que $a = 258$ e $b = 60$. Logo:

(1) Dividindo $a = 258$ por $b = 60$, temos o resto $r_1 = 18$.
(2) Dividindo $b = 60$ por $r_1 = 18$, temos o resto $r_2 = 6$.
(3) Dividindo $r_1 = 18$ por $r_2 = 6$, temos o resto $r_3 = 0$.

Assim, $r_2 = 6 = \text{MDC}(258, 60)$.

O algoritmo euclidiano é uma maneira muito eficiente para encontrar o máximo divisor comum de dois inteiros positivos a e b. O fato de que o algoritmo termina, segue de (*). O fato de que o algoritmo resulta em $d = \text{MDC}(a, b)$ não é óbvio; isso é discutido na Seção 11.6.

3.9 COMPLEXIDADE DE ALGORITMOS

A análise de algoritmos é uma tarefa fundamental em ciência da computação. Para comparar algoritmos, devemos ter alguns critérios para medir a eficiência deles. Essa seção discute esse importante tópico.

Suponha que M é um algoritmo e que n é o tamanho dos dados de entrada. O tempo e o espaço usados pelo algoritmo são as duas principais medidas da eficiência de M. O tempo é medido pela contagem do número de "operações-chave"; por exemplo:

(a) Em classificação e busca, conta-se o número de comparações.
(b) Em aritmética, conta-se multiplicações e se negligencia adições.

Operações-chave são assim definidas quando o tempo para as demais operações é muito menor ou, pelo menos, proporcional ao tempo para as operações-chave. O espaço é medido, contando-se o máximo de memória necessária para o algoritmo.

A *complexidade* de um algoritmo M é a função $f(n)$ que fornece o tempo de processamento e/ou a demanda por espaço de armazenamento do algoritmo em termos do tamanho n dos dados de entrada. Frequentemente, o espaço de armazenamento exigido por um algoritmo é simplesmente um múltiplo do tamanho dos dados. Consequentemente, a não ser que seja estabelecido ou sugerido o contrário, o termo "complexidade" deve se referir ao tempo de processamento do algoritmo.

A função de complexidade $f(n)$, que assumimos fornecer o tempo de processamento de um algoritmo, em geral depende não apenas do tamanho n dos dados de entrada, mas também dos dados em particular. Por exemplo,

suponha que queremos buscar em um conto TEXT, escrito em inglês, a primeira ocorrência de uma dada palavra W de três letras. Claramente, se W for a palavra de três letras "the" (artigo definido, "o", "a", "os", "as"), então W provavelmente ocorre próxima do início de TEXT e, assim, $f(n)$ é pequena. Por outro lado, se W é a palavra de três letras "zoo" (substantivo, "zoológico"), então W pode não aparecer em TEXT e, assim, $f(n)$ é grande.

A discussão acima nos conduz à questão de determinar a função de complexidade $f(n)$ para certos casos. Os dois casos que normalmente se investigam na teoria de complexidade são os seguintes:

(1) *Pior caso*: O valor máximo de $f(n)$ para qualquer entrada possível.

(2) *Caso médio*: O valor esperado de $f(n)$.

A análise do caso médio assume uma certa distribuição probabilística para os dados de entrada, uma hipótese pode ser as permutações possíveis de um conjunto de dados serem igualmente prováveis. O caso médio também emprega o conceito a seguir de teoria de probabilidades. Suponha que os números $n_1, n_2, \ldots, n_k$ ocorram com probabilidades respectivas $p_1, p_2, \ldots, p_k$. Então o *valor esperado* ou *médio E* é dado por

$$E = n_1 p_1 + n_2 p_2 + \cdots + n_k p_k$$

Essas ideias são ilustradas abaixo.

Busca linear

Suponha que uma sequência linear de dados DATA contém n elementos, e que um ITEM específico de informação seja dado. Queremos encontrar a localização LOC de ITEM na sequência DATA ou enviar alguma mensagem, como LOC = 0, para indicar que ITEM não aparece em DATA. O algoritmo de busca linear resolve esse problema comparando ITEM com cada elemento de DATA, um a um. Ou seja, comparamos ITEM com DATA[1], então com DATA[2], e assim por diante, até encontrarmos LOC tal que ITEM = DATA[LOC].

A complexidade do algoritmo de busca é dada pelo número C de comparações entre ITEM e DATA[K]. Buscamos $C(n)$ para o pior caso e o caso médio.

(1) ***Pior caso***: Claramente, o pior caso ocorre quando ITEM é o último elemento na sequência DATA ou simplesmente não está lá. Em qualquer situação temos

$$C(n) = n$$

Consequentemente, $C(n) = n$ é a complexidade do pior caso do algoritmo de busca linear.

(2) ***Caso médio***: Aqui assumimos que ITEM aparece em DATA e que é igualmente provável sua ocorrência em qualquer posição da sequência. Consequentemente, o número de comparações pode ser qualquer um dos números $1, 2, 3, \ldots, n$, e cada número ocorre com probabilidade $p = 1/n$. Então

$$\begin{aligned} C(n) &= 1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} + \cdots + n \cdot \frac{1}{n} \\ &= (1 + 2 + \cdots + n) \cdot \frac{1}{n} \\ &= \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2} \end{aligned}$$

Isso está de acordo com nossa intuição de que o número médio de comparações necessárias para encontrar a localização de ITEM é aproximadamente igual à metade do número de elementos na lista DATA.

Observação: A complexidade do caso médio de um algoritmo é geralmente muito mais complicada para analisar do que aquela do pior caso. Além disso, a distribuição probabilística que se assume para o caso médio pode não se aplicar a situações reais. Logo, a menos que seja estabelecido ou sugerido o contrário, a complexidade de um algoritmo deve significar a função que fornece o tempo de processamento do pior caso em termos de tamanho da entrada. Essa não é uma hipótese muito forte, uma vez que a complexidade do caso médio para muitos algoritmos é proporcional ao pior caso.

Taxa de crescimento; notação *O* maiúsculo

Suponha que M é um algoritmo e que n é o tamanho dos dados de entrada. Claramente, a complexidade $f(n)$ de M aumenta à medida que n cresce. De modo geral, é a taxa de crescimento de $f(n)$ que desejamos examinar. Isso é feito comparando $f(n)$ com alguma função padrão, como

$$\log n, \quad n, \quad n \log n, \quad n^2, \quad n^3, \quad 2^n$$

As taxas de crescimento para essas funções padrão são indicadas na Fig. 3-7, que nos fornece seus valores aproximados para certos valores de n. Observe que as funções são listadas em ordem de suas taxas de crescimento: a função logarítmica $\log_2 n$ cresce mais lentamente, a exponencial 2^n, mais rapidamente, e as funções polinomiais crescem de acordo com o expoente c.

n \ $g(n)$	$\log n$	n	$n \log n$	n^2	n^3	2^n
5	3	5	15	25	125	32
10	4	10	40	100	10^3	10^3
100	7	100	700	10^4	10^6	10^{30}
1000	10	10^3	10^4	10^6	10^9	10^{300}

Figura 3-7 Taxa de crescimento de funções padrão.

A maneira como comparamos nossa função de complexidade $f(n)$ com as funções padrão é usando a notação "*O* maiúsculo" que formalmente se define abaixo.

Definição 3.4: Sejam $f(x)$ e $g(x)$ funções arbitrárias definidas sobre **R** ou um subconjunto de **R**. Dizemos que "$f(x)$ é de ordem $g(x)$" e escrevemos

$$f(x) = O(g(x))$$

se existe um número real k e uma constante positiva C tais que, para todo $x > k$, temos

$$|f(x)| \leq C|g(x)|$$

Em outras palavras, $f(x) = O(g(x))$ se uma constante múltipla de $|g(x)|$ excede $|f(x)|$ para todo x maior do que algum número real k.

Também escrevemos

$$f(x) = h(x) + O(g(x)) \quad \text{quando} \quad f(x) - h(x) = O(g(x))$$

(Essa é a chamada notação "*O* maiúsculo", uma vez que $f(x) = o(g(x))$ tem um significado totalmente diferente.)

Considere agora um polinômio $P(x)$ de grau m. Mostramos no Problema 3.24 que $P(x) = O(x^m)$. Assim, por exemplo,

$$7x^2 - 9x + 4 = O(x^2) \quad \text{e} \quad 8x^3 - 576x^2 + 832x - 248 = O(x^3)$$

Complexidade de algoritmos bem conhecidos

Assumindo que $f(n)$ e $g(n)$ são funções definidas sobre os inteiros positivos, então

$$f(n) = O(g(n))$$

significa que $f(n)$ é cotada por uma constante múltipla de $g(n)$ para quase todo n.

Para indicar a conveniência dessa notação, mostramos a complexidade de certos algoritmos bem conhecidos de busca e classificação em ciência da computação:

(a) Busca linear: $O(n)$ (c) Classificação de bolhas: $O(n^2)$

(b) Busca binária: $O(\log n)$ (d) Ordenação por mistura: $O(n \log n)$

Problemas Resolvidos

Funções

3.1 Seja $X = \{1, 2, 3, 4\}$ Determine se cada relação sobre X é uma função de X em X

(*a*) $f = \{(2, 3), (1, 4), (2, 1), (3, 2), (4, 4)\}$

(*b*) $g = \{(3, 1), (4, 2), (1, 1)\}$

(*c*) $h = \{(2, 1), (3, 4), (1, 4), (2, 1), (4, 4)\}$

Lembre que um subconjunto f de $X \times X$ é uma função $f : X \to X$ se, e somente se, cada $a \in X$ aparece como a primeira coordenada em exatamente um par ordenado de f.

(a) Não. Dois pares ordenados diferentes $(2, 3)$ e $(2, 1)$ em f têm o mesmo número 2 como suas primeiras coordenadas.

(b) Não. O elemento $2 \in X$ não aparece como a primeira coordenada em qualquer par ordenado de g.

(c) Sim. Apesar de $2 \in X$ aparecer como a primeira coordenada em dois pares ordenados de h, eles são iguais.

3.2 Esboce o gráfico de: (*a*) $f(x) = x^2 + x - 6$; (*b*) $g(x) = x^3 - 3x^2 - x + 3$.

Faça uma tabela de valores para x e encontre os valores correspondentes da função. Como as funções são polinomiais, plote os pontos em diagrama coordenado e então desenhe uma curva contínua e suave através dos pontos. Ver Fig. 3-8

x	$f(x)$
−4	6
3	0
−2	4
−1	6
0	−6
1	−4
2	0
3	6

x	$g(x)$
−2	−15
−1	0
0	3
1	0
2	3
3	0
4	15

Gráfico de $f = x^2 + x - 6$ — Gráfico de $g = x^3 - 3x^2 - x + 3$

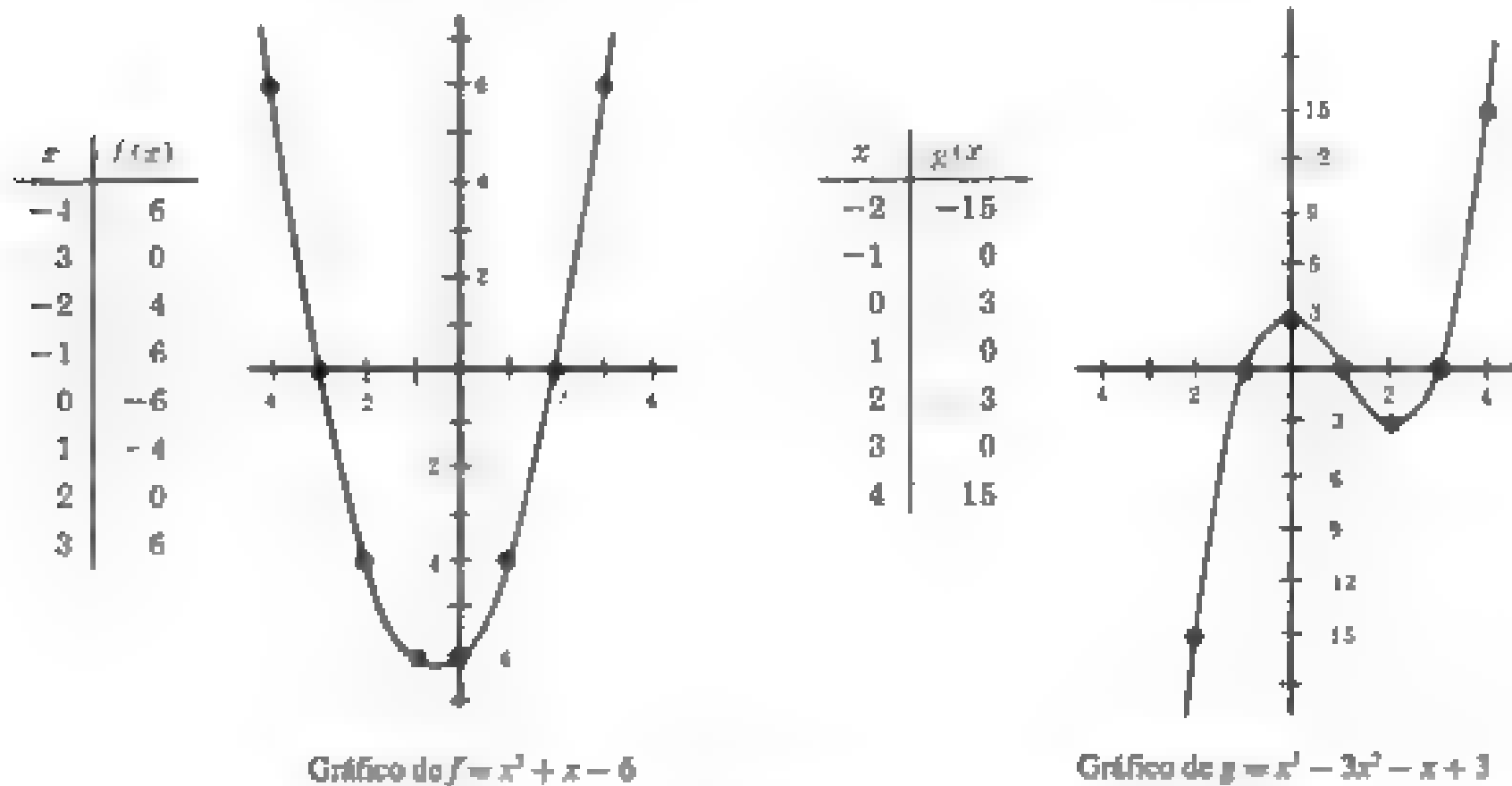



Figura 3-8

3.3 Sejam $A = \{a, b, c\}$, $B = \{x, y, z\}$, $C = \{r, s, t\}$ Considere $f : A \to B$ e $g : B \to C$ definidas por:

$$f = \{(a, y)(b, x), (c, y)\} \quad \text{e} \quad g = \{(x, s), (y, t), (z, r)\}$$

Encontre: (*a*) a função composta $g \circ f : A \to C$; (*b*) $\text{Im}(f)$, $\text{Im}(g)$, $\text{Im}(g \circ f)$.

(*a*) Use a definição de composição de funções para calcular:

$$(g \circ f)(a) = g(f(a)) = g(y) = t$$
$$(g \circ f)(b) = g(f(b)) = g(x) = s$$
$$(g \circ f)(c) = g(f(c)) = g(y) = t$$

Isto é, $g \circ f = \{(a, t), (b, s), (c, t)\}$.

(b) Encontre as imagens (ou segundas coordenadas):

$$\text{Im}(f) = \{x, y\}, \quad \text{Im}(g) = \{r, s, t\}, \quad \text{Im}(g \circ f) = \{s, t\}$$

3.4 Sejam $f: \mathbf{R} \rightarrow \mathbf{R}$ e $g: \mathbf{R} \rightarrow \mathbf{R}$ definidas por $f(x) = 2x + 1$ e $g(x) = x^2 - 2$. Encontre a fórmula para a função composta $g \circ f$.

Calcule $g \circ f$ como se segue: $(g \circ f)(x) = g(f(x)) = g(2x + 1) = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$.

Observe que a mesma resposta pode ser encontrada escrevendo

$$y = f(x) = 2x + 1 \quad \text{e} \quad z = g(y) = y^2 - 2$$

e então eliminando y de ambas as equações:

$$z = y^2 - 2 = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$$

Funções injetoras, sobrejetoras e inversíveis

3.5 Sejam as funções $f: A \rightarrow B$, $g: B \rightarrow C$ e $h: C \rightarrow D$ definidas pela Fig. 3-9. Determine se cada função é: (*a*) sobrejetora, (*b*) injetora, (*c*) inversível.

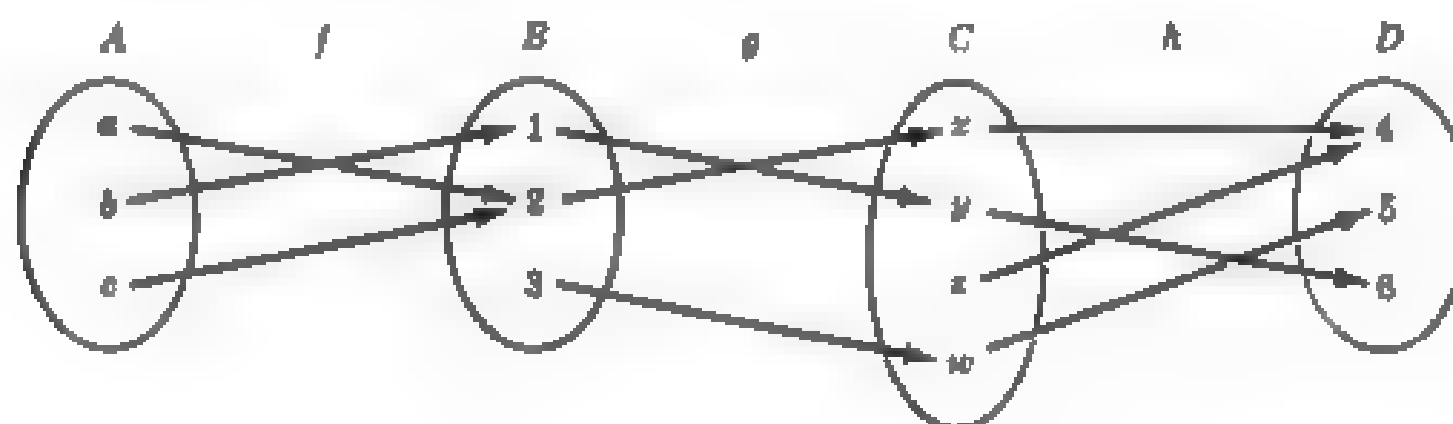



Figura 3-9

(*a*) A função $f: A \rightarrow B$ não é sobrejetora, pois $3 \in B$ não é a imagem de qualquer elemento em A.

A função $g: B \rightarrow C$ não é sobrejetora, pois $z \in C$ não é a imagem de qualquer elemento de B.

A função $h: C \rightarrow D$ é sobrejetora, pois cada elemento em D é a imagem de algum elemento de C.

(*b*) A função $f: A \rightarrow B$ não é injetora, uma vez que a e c têm a mesma imagem 2.

A função $g: B \rightarrow C$ é injetora, uma vez que 1, 2 e 3 têm imagens distintas.

A função $h: C \rightarrow D$ não é injetora, uma vez que x e z têm a mesma imagem 4.

(*c*) Nenhuma função é injetora e sobrejetora, logo, nenhuma delas é inversível.

3.6 Considere permutações $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}$ em S_6.

Encontre: (*a*) a composição $\tau \circ \sigma$; (*b*) σ^{-1}.

(a) Note que σ leva 1 em 3 e τ leva 3 em 6. Assim, a composição $\tau \circ \sigma$ leva 1 em 6. Isto é, $(\tau \circ \sigma)(1) = 6$. Além disso, $\tau \circ \sigma$ leva 2 em 6 em 1, ou seja, $(\tau \circ \sigma)(2) = 1$. Analogamente,

$$(\tau \circ \sigma)(3) = 5, \quad (\tau \circ \sigma)(4) = 3, \quad (\tau \circ \sigma)(5) = 2, \quad (\tau \circ \sigma)(6) = 4$$

Logo,

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 3 & 2 & 4 \end{pmatrix}$$

(b) Procure 1 na segunda linha de σ. Note que σ leva 5 em 1. Logo, $\sigma^{-1}(1) = 5$. Procure 2 na segunda linha de σ. Observe que σ leva 6 em 2. Portanto, $\sigma^{-1}(2) = 6$. Analogamente, $\sigma^{-1}(3) = 1$, $\sigma^{-1}(4) = 3$, $\sigma^{-1}(5) = 4$, $\sigma^{-1}(6) = 2$. Assim,

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 3 & 4 & 2 \end{pmatrix}$$

3.7 Considere as funções $f: A \to B$ e $g: B \to C$. Prove o seguinte:

(a) Se f e g são injetoras, então a função composta $g \circ f$ é injetora.

(b) Se f e g são sobrejetoras, então $g \circ f$ é sobrejetora.

(a) Suponha que $(g \circ f)(x) = (g \circ f)(y)$, então $g(f(x)) = g(f(y))$. Logo, $f(x) = f(y)$ porque g é injetora. Além disso, $x = y$, uma vez que f é injetora. Consequentemente, $g \circ f$ é injetora.

(b) Seja c um elemento arbitrário qualquer de C. Como g é sobrejetora, existe um $b \in B$ tal que $g(b) = c$. Como f é sobrejetora, existe um $a \in A$ tal que $f(a) = b$. Mas então

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

Logo, cada $c \in C$ é a imagem de algum elemento $a \in A$. Consequentemente, $g \circ f$ é uma função sobrejetora.

3.8 Seja $f: \mathbf{R} \to \mathbf{R}$ definida por $f(x) = 2x - 3$. Logo, f é injetora e sobrejetora e, portanto, f admite uma função inversa f^{-1}. Encontre uma fórmula para f^{-1}.

Seja y a imagem de x sob a função f.

$$y = f(x) = 2x - 3$$

Consequentemente, x é a imagem de y sob a função inversa f^{-1}. Resolva para x em termos de y na equação acima.

$$x = (y + 3)/2$$

Então $f^{-1}(y) = (y + 3)/2$. Substitua y por x para obter

$$f^{-1}(x) = \frac{x+3}{2}$$

que é a fórmula para f^{-1}, utilizando a variável independente usual x.

3.9 Prove a seguinte generalização da Lei de DeMorgan. Para qualquer classe de conjuntos $\{A_i\}$, temos

$$(\cup_i A_i)^c = \cap_i A_i^c$$

Sabemos que

$$x \in (\cup_i A_i)^c \quad \text{sss } x \notin \cup_i A_i, \quad \text{sss } \forall_i \in I, x \notin A_i, \quad \text{sss } \forall_i \in I, x \in A_i^c, \text{sss } x \in \cap_i A_i^c$$

Portanto, $(\cup_i A_i)^c = \cap_i A_i^c$. (Aqui usamos as notações lógicas "sss" para "se, e somente se," e $\forall$ para "para todo".)

Cardinalidade

3.10 Encontre o número cardinal de cada conjunto:

(*a*) $A = \{a, b, c, \ldots, y, z\}$, (c) $C = \{10, 20, 30, 40, \ldots\}$,

(*b*) $B = \{x \mid x \in \mathbf{N}, x^2 = 5\}$, (d) $D = \{6, 7, 8, 9, \ldots\}$.

(*a*) $|A| = 26$, pois há 26 elementos no alfabeto inglês.

(*b*) $|B| = 0$, uma vez que não existe inteiro positivo cujo quadrado é 5, ou seja, B é vazio.

(*c*) $|C| = \aleph_0$, pois $f: \mathbf{N} \to C$, definida por $f(n) = 10_n$, é uma correspondência um para um entre $\mathbf{N}$ e C.

(*d*) $|D| = \aleph_0$, uma vez que $g: \mathbf{N} \to D$, definida por $g(n) = n + 5$, é uma correspondência um para um entre $\mathbf{N}$ e D.

3.11 Mostre que o conjunto dos $\mathbf{Z}$ inteiros tem cardinalidade $\aleph_0$.

O diagrama a seguir mostra uma correspondência um para um entre $\mathbf{N}$ e $\mathbf{Z}$.

$$\begin{array}{ccccccccc} \mathbf{N} = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \mathbf{Z} = & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 \end{array}$$

Ou seja, a função $f: \mathbf{N} \to \mathbf{Z}$ a seguir é injetora e sobrejetora:

$$f(n) = \begin{cases} n/2 & \text{se } n \text{ é par} \\ (1 - n)/2 & \text{se } n \text{ é ímpar} \end{cases}$$

Consequentemente, $|\mathbf{Z}| = |\mathbf{N}| = \aleph_0$.

3.12 Seja $A_1, A_2, \ldots$ uma quantia contável de conjuntos finitos. Prove que a união $S = \cup_i A_i$ é contável.

Listamos primeiro os elementos de A_1, em seguida, os elementos de A_2 que não pertencem a A_1, depois, os elementos de A_3 que não pertencem a A_1 ou A_2, isto é, que já não tenham sido listados, e assim por diante. Como os A_i são finitos, sempre podemos listar os elementos de cada conjunto. Esse processo é formalmente executado como se segue.

Primeiro definimos conjuntos $B_1, B_2, \ldots$, onde B_i contém os elementos de A_i que não pertencem aos conjuntos anteriores, ou seja, definimos

$$B_1 = A_1 \quad \text{e} \quad B_k = A_k \setminus (A_1 \cup A_2 \cup \cdots \cup A_{k-1})$$

Logo, os B_i são disjuntos e $S = \cup_i B_i$. Sejam $b_{i1}, b_{i2}, \ldots, b_{im_i}$ os elementos de B_i. Então $S = \{b_{ij}\}$. Seja $f: S \to \mathbf{N}$ definida como:

$$f(b_{ij}) = m_1 + m_2 + \cdots + m_{i-1} + j$$

Se S é finito, então S é contável. Se S é infinito, então f é uma correspondência um para um entre S e $\mathbf{N}$. Logo, S é contável.

3.13 Prove o Teorema 3.2. Uma união contável de conjuntos contáveis é contável.

Suponha que $A_1, A_2, A_3, \ldots$ são uma quantia contável de conjuntos contáveis. Especificamente, suponha que $a_{i1}, a_{i2}, a_{i3}, \ldots$ são os elementos de A_i. Defina conjuntos $B_2, B_3, B_4, \ldots$ como se segue.

$$Bk = \{a_{ij} \mid i + j = k\}$$

Por exemplo, $B_6 = \{a_{15}, a_{24}, a_{33}, a_{42}, a_{51}\}$. Observe que cada B_k é finito e que

$$S = \cup_i A_i = \cup_k B_k$$

Pelo problema anterior, $\cup_k B_k$ é contável. Logo, $S = \cup_i A_i$ é contável e o teorema está demonstrado.

3.14 Demonstre o Teorema 3.3. O conjunto I de todos os números reais entre 0 e 1 (inclusive) é não contável.

O conjunto I é claramente infinito, uma vez que ele contém $1, \frac{1}{2}, \frac{1}{3}, \ldots$. Suponha que I é enumerável. Então existe uma correspondência um para um $f: N \to \mathbf{I}$. Sejam $f(1) = a_1, f(2) = a_2, \ldots$, ou seja, $\mathbf{I} = \{a_1, a_2, a_3, \ldots\}$. Listamos os elementos $a_1, a_2, a_3, \ldots$ em uma coluna e expressamos cada um em sua expansão decimal.

$$\begin{aligned} a_1 &= 0.x_{11}x_{12}x_{13}x_{14}\ldots \\ a_2 &= 0.x_{21}x_{22}x_{23}x_{24}\ldots \\ a_3 &= 0.x_{31}x_{32}x_{33}x_{34}\ldots \\ a_4 &= 0.x_{41}x_{42}x_{43}x_{44}\ldots \\ &\ldots \end{aligned}$$

onde $x_{ij} \in \{0, 1, 2, \ldots, 9\}$. (Para aqueles números que podem ser expressos em duas expansões decimais distintas, por exemplo, $0{,}2000000\ldots = 0{,}1999999\ldots$, escolhemos a expansão que termina com os números nove.)

Seja $b = 0{,}y_1y_2y_3y_4\ldots$ o número real obtido como se segue

$$y_i = \begin{cases} 1 & \text{se } x_{ii} \neq 1 \\ 2 & \text{se } x_{ii} = 1 \end{cases}$$

Logo, $b \in \mathbf{I}$. Mas

$$\begin{aligned} b \neq a_1 &\text{ porque } y_1 \neq x_{11} \\ b \neq a_2 &\text{ porque } y_2 \neq x_{22} \\ b \neq a_3 &\text{ porque } y_3 \neq x_{33} \end{aligned}$$

Portanto, b não pertence a $\mathbf{I} = \{a_1, a_2, \ldots\}$. Isso contradiz o fato de que $b \in \mathbf{I}$. Logo, a suposição de que $\mathbf{I}$ é enumerável deve ser falsa e, assim, $\mathbf{I}$ é não contável.

Funções matemáticas especiais

3.15 Encontre: (*a*) $\lfloor 7{,}5 \rfloor$, $\lfloor -7{,}5 \rfloor$, $\lfloor -18 \rfloor$; (*b*) $\lceil 7{,}5 \rceil$, $\lceil -7{,}5 \rceil$, $\lceil -18 \rceil$.

(*a*) Por definição, $\lfloor x \rfloor$ denota o maior inteiro que não excede x, logo, $\lfloor 7{,}5 \rfloor = 7$, $\lfloor -7{,}5 \rfloor = -8$, $\lfloor -18 \rfloor = -18$.

(*b*) Por definição, $\lceil x \rceil$ denota o menor inteiro que não é menor do que x, portanto, $\lceil 7{,}5 \rceil = 8$, $\lceil -7{,}5 \rceil = -7$, $\lceil -18 \rceil = -18$

3.16 Determine (*a*) 25 (mod7); (*b*) 25 (mod5), (*c*) −35 (mod 11), (*d*) −3 (mod 8).

Quando k é positivo, simplesmente divida k pelo módulo M para obter o resto r. Então, $r = k(\text{mod } M)$. Se k é negativo, divida $|k|$ por M para obter o resto r'. Então, $k \text{ (mod } M) = M - r'$ (quando $r' \neq 0$). Assim

(*a*) $25 \text{ (mod } 7) = 4$ (*c*) $-35 \text{ (mod } 11) = 11 - 2 = 9$

(*b*) $25 \text{ (mod } 5) = 0$ (*d*) $-3 \text{ (mod } 8) = 8 - 3 = 5$

3.17 Calcule, módulo $M = 15$, o que se segue: (*a*) $9 + 13$; (*b*) $7 + 11$, (*c*) $4 - 9$; (*d*) $2 - 10$.

Use $a \pm M = a(\text{mod } M)$.

(*a*) $9 + 13 = 22 = 22 - 15 = 7$ (*c*) $4 - 9 = -5 = -5 + 15 = 10$

(*b*) $7 + 11 = 18 = 18 - 15 = 3$ (*d*) $2 - 10 = -8 = -8 + 15 = 7$

3.18 Simplifique: (*a*) $\dfrac{n!}{(n-1)!}$; (*b*) $\dfrac{(n+2)!}{n!}$.

(*a*) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{(n-1)(n-2)\cdots 3\cdot 2\cdot 1} = n$ ou, simplesmente, $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n$

(*b*) $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n!}{n!} = (n+2)(n+1) = n^2 + 3n + 2$

3.19 Calcule: (*a*) $\log_2 8$; (*b*) $\log_2 64$, (*c*) $\log_{10} 100$; (*d*) $\log_{10} 0{,}001$.

(*a*) $\log_2 8 = 3$, pois $2^3 = 8$ (*c*) $\log_{10} 100 = 2$, pois $10^2 = 100$

(*b*) $\log_2 64 = 6$, pois $2^6 = 64$ (*d*) $\log_{10} 0{,}001 = -3$, pois $10^{-3} = 0{,}001$

Funções recursivas

3.20 Sejam a e b inteiros positivos, e suponha que Q é recursivamente definida como se segue.

$$Q(a, b) = \begin{cases} 0 & \text{se } a < b \\ Q(a - b, b) + 1 & \text{se } b \leq a \end{cases}$$

(*a*) Encontre: (i) $Q(2, 5)$; (ii) $Q(12, 5)$.

(*b*) O que essa função Q faz? Calcule $Q(5861, 7)$.

(*a*) (i) $Q(2, 5) = 0$, uma vez que $2 < 5$.

(ii) $Q(12, 5) = Q(7, 5) + 1$

$= [Q(2, 5) + 1] + 1 = Q(2, 5) + 2$

$= 0 + 2 = 2$

(b) Cada vez que b é subtraído de a, o valor de Q é acrescentado de 1. Logo, $Q(a, b)$ encontra o quociente, quando a é dividido por b. Assim, $Q(5861, 7) = 837$

3.21 Use a definição da função de Ackermann para encontrar $A(1, 3)$.

A Fig. 3-10 mostra os 15 passos que são usados para calcular $A(1, 3)$.

O deslocamento para a direita indica que estamos adiando um cálculo e chamando novamente a definição, o deslocamento para a esquerda indica que estamos retornando. Observe que o item (*a*) da definição é usado nos Passos 5, 8, 11 e 14; (*b*) no Passo 4, (*c*) nos Passos 1, 2 e 3. Nos demais passos, estamos retornando com substituições.

(1)	$A(1, 3) = A(0, A(1, 2))$	(9)	$A(1, 1) = 3$
(2)	$A(1, 2) = A(0, A(1, 1))$	(10)	$A(1, 2) = A(0, 3)$
(3)	$A(1, 1) = A(0, A(1, 0))$	(11)	$A(0, 3) = 3 + 1 = 4$
(4)	$A(1, 0) = A(0, 1)$	(12)	$A(1, 2) = 4$
(5)	$A(0, 1) = 1 + 1 = 2$	(13)	$A(1, 3) = A(0, 4)$
(6)	$A(1, 0) = 2$	(14)	$A(0, 4) = 4 + 1 = 5$
(7)	$A(1, 1) = A(0, 2)$	(15)	$A(1, 3) = 5$
(8)	$A(0, 2) = 2 + 1 = 3$		

Figura 3-10

Problemas variados

3.22 Determine o domínio D de cada uma das seguintes funções reais de uma variável real.

(*a*) $f(x) = \frac{1}{x-2}$ (*c*) $f(x) = \sqrt{25 - x^2}$

(*b*) $f(x) = x^2 - 3x - 4$ (*d*) x^2, onde $0 \leq x \leq 2$

Quando uma função real de uma variável real é dada por uma fórmula $f(x)$, então o domínio D consiste no maior subconjunto de $\mathbf{R}$ para o qual $f(x)$ tem significado e é real, a menos que seja especificado o contrário.

(a) f não é definida para $x - 2 = 0$, ou seja, para $x = 2$; logo, $D = \mathbf{R}\setminus\{2\}$.

(b) f é definida para todo número real, logo, $D = \mathbf{R}$.

(c) f não é definida quando $25 - x^2$ é negativo; logo, $D = [-5, 5] = \{x \mid -5 \leq x \leq 5\}$

(d) Aqui o domínio de f é explicitamente dado como $D = \{x \mid 0 \leq x \leq 2\}$.

3.23 Para qualquer $n \in \mathbf{N}$, seja $D_n = (0, 1/n)$, o intervalo aberto de 0 a $1/n$. Encontre.

(*a*) $D_3 \cup D_4$; (*b*) $D_3 \cap D_{20}$; (*c*) $D_s \cup D_t$; (*d*) $D_s \cap D_t$.

(*a*) Como $(0, 1/3)$ é um conjunto tal que o segundo é subconjunto do primeiro, $(0, 1/7)$, $D_3 \cup D_4 = D_3$.

(*b*) Como $(0, 1/20)$ é um subconjunto de $(0, 1/3)$, $D_3 \cap D_{20} = D_{20}$.

(*c*) Seja $m = \min(s, t)$, isto é, o menor entre os dois números s e t; então D_m é igual a D_s, ou D_t contém o outro como subconjunto. Logo, $D_s \cap D_t = D_m$.

(*d*) Seja $M = \max(s, t)$, isto é, o maior entre os dois números s e t; então $D_s \cap D_t = D_M$.

3.24 Suponha que $P(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_m n^m$ tem grau m. Prove que $P(n) = O(n^m)$.

Seja $b_0 = |a_0|$, $b_1 = |a_1|, \ldots, b_m = |a_m|$. Então, para $n \geq 1$,

$$p(n) \leq b_0 + b_1 n + b_2 n^2 + \cdots + b_m n^m = \left(\frac{b_0}{n^m} + \frac{b_1}{n^{m-1}} + \cdots + b_m\right) n^m$$
$$\leq (b_0 + b_1 + \cdots + b_m) n^m = M n^m$$

onde $M = |a_0| + |a_1| + \cdots + |a_m|$. Logo, $P(n) = O(n^m)$.

Por exemplo, $5x^3 + 3x = O(x^3)$ e $x^5 - 4000000x^2 = O(x^5)$.

3.25 Demonstre o Teorema 3.4 (Cantor): $|A| < |\text{Potência}(A)|$ (onde Potência (A) é o conjunto potência de A).

A função $g: A \to \text{Potência}(A)$ definida por $g(a) = \{a\}$ é claramente bijetora; logo $|A| \leq |\text{Potência}(A)|$.

Se mostrarmos que $|A| \neq |\text{Potência}(A)|$, então o teorema é consequência. Suponha o contrário, ou seja, suponha que $|A| = |\text{Potência}(A)|$ e que $f: A \to \text{Potência}(A)$ é uma função que é injetora e sobrejetora. Considere que $a \in A$ é um "mau" elemento se $a \notin f(a)$, e seja B o conjunto de maus elementos. Em outras palavras,

$$B = \{x : x \in A, x \notin f(x)\}$$

Logo, B é um subconjunto de A. Como $f: A \to \text{Potência}(A)$ é sobrejetora, existe $b \in A$ tal que $f(b) = B$. É b um "mau" elemento ou um "bom" elemento? Se $b \in B$, então, pela definição de B, $b \notin f(b) = B$, o que é impossível. Analogamente, se $b \notin B$, então $b \in f(b) = B$, o que também é impossível. Logo, a hipótese original de que $|A| = |\text{Potência}(A)|$ conduz a uma contradição. Assim, a hipótese é falsa e, portanto, o teorema é verdadeiro.

3.26 Prove a formulação equivalente ao Teorema 3.5 de Schroeder-Bernstein dada a seguir:

Suponha que $X \supseteq Y \supseteq X_1$ e $X \simeq X_1$. Então, $X \simeq Y$.

Como $X \simeq X_1$, existe uma correspondência um para um (bijeção) $f: X \to X_1$. Uma vez que $X \supset Y$, a restrição de f a Y, que também denotamos por f, é novamente um para um. Seja $f(Y) = Y_1$. Então Y e Y_1 são equipotentes,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1$$

e $f: Y \to Y_1$ é bijetora. Mas agora $Y \supseteq X_1 \supseteq Y_1$ e $Y \simeq Y_1$. Por motivos semelhantes, X_1 e $f(X_1) = X_2$ são equipotentes,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2$$

e $f: X \to X_2$ é bijetora. Consequentemente, existem conjuntos equipotentes $X, X_1, X_2, \ldots$ e conjuntos equipotentes $Y, Y_1, Y_2, \ldots$ tais que

$$X \supset Y \supset X_1 \supset Y_1 \supset X_2 \supset Y_2 \supset X_3 \supset Y_3 \supset \cdots$$

e $f: X_k \to X_{k+1}$ e $f: Y_k \to Y_{k+1}$ são bijetoras.

Faça

$$B = X \cap Y \cap X_1 \cap Y_1 \cap X_2 \cap Y_2 \cap \cdots$$

Então

$$X = (X \setminus Y) \cup (Y \setminus X_1) \cup (X_1 \setminus Y_1) \cup \cdots \cup B$$

$$Y = (Y \setminus X_1) \cup (X_1 \setminus Y_1) \cup (Y_1 \setminus X_2) \cup \cdots \cup B$$

Além disso, $X \setminus Y, X_1 \setminus Y_1, X_2 \setminus Y_2, \ldots$ são equipotentes. De fato, a função

$$f: (X_k \setminus Y_k) \to (X_{k+1} \setminus Y_{k+1})$$

é injetora e sobrejetora.

Considere a função $g: X \to Y$ definida pelo diagrama na Fig. 3-11. Ou seja,

$$g(x) = \begin{cases} f(x) & \text{se } x \in X_k \setminus Y_k \text{ ou } x \in X \setminus Y \\ x & \text{se } x \in Y_k \setminus X_k \text{ ou } x \in B \end{cases}$$

Então g é injetora e sobrejetora. Portanto, $X \simeq Y$.

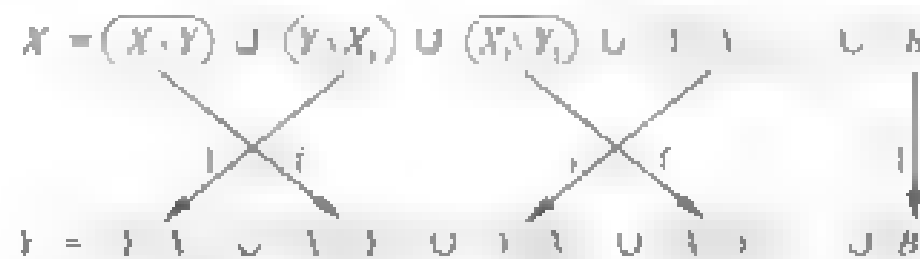



Figura 3-11

Problemas Complementares

Funções

3.27 Seja $W = \{a, b, c, d\}$. Decida se cada conjunto de pares ordenados é uma função de W em W.

(a) $\{(b, a), (c, d), (d, a), (c, d), (a, d)\}$ (c) $\{(a, b), (b, b), (c, d), (d, b)\}$

(b) $\{(d, d), (c, a), (a, b), (d, b)\}$ (d) $\{(a, a), (b, a), (a, b), (c, d)\}$

3.28 Seja $V = \{1, 2, 3, 4\}$. Para as seguintes funções $f: V \to V$ e $g: V \to V$ encontre:

(a) $f \circ g$, (b), $g \circ f$, (c) $f \circ f$

$$f = \{(1, 3), (2, 1), (3, 4), (4, 3)\} \quad \text{e} \quad g = \{(1, 2), (2, 3), (3, 1), (4, 1)\}$$

3.29 Encontre a composição $h \circ g \circ f$ para as funções da Fig. 3-9.

Funções injetoras, sobrejetoras e inversíveis

3.30 Determine se cada função é injetora.

(a) Para cada pessoa na Terra, designe o número que corresponde à sua idade.

(b) Para cada país no mundo, assinale a latitude e a longitude de sua capital.

(c) Para cada livro escrito por um único autor, assinale o autor.

(d) Para cada país no mundo que tem um primeiro-ministro, corresponda seu primeiro-ministro.

3.31 Faça funções f, g e h de $V = \{1, 2, 3, 4\}$ em V serem definidas por $f(n) = 6 - n$, $g(n) = 3$ e $h = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$. Decida quais funções são:

(a) injetoras; (b) sobrejetoras; (c) ambos os casos; (d) nenhum dos casos.

3.32 Faça funções f, g e h de $\mathbf{N}$ em $\mathbf{N}$ serem definidas por $f(n) = n + 2$, (b) $g(n) = 2^n$ e $h(n)$ = número de divisores positivos de n. Decida quais funções são:

(a) injetoras; (b) sobrejetoras; (c) ambos os casos, (d) nenhum dos casos, (e) Encontre $h'(2) = \{x | h(x) = 2\}$

3.33 Decida quais das seguintes funções são: (a) injetoras; (b) sobrejetoras; (c) ambos os casos; (d) nenhum dos casos.

(1) $f: \mathbf{Z}^2 \to \mathbf{Z}$, onde $f(n, m) = n - m$; (3) $h: \mathbf{Z} \times (\mathbf{Z} \backslash 0) \to \mathbf{Q}$, onde $h(n, m) = n/m$;

(2) $g: \mathbf{Z}^2 \to \mathbf{Z}^2$, onde $g(n, m) = (m, n)$; (4) $k: \mathbf{Z} \to \mathbf{Z}^2$, onde $k(n) = (n, n)$.

3.34 Seja $f: \mathbf{R} \to \mathbf{R}$ definida por $f(x) = 3x - 7$. Encontre uma fórmula para a função inversa $f^{-1}: \mathbf{R} \to \mathbf{R}$.

3.35 Considere permutações $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 1 & 3 & 4 \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 2 & 5 \end{pmatrix}$ em S_6.

Encontre: (a) $\tau \circ \sigma$; (b) $\sigma \circ \tau$; (c) σ^2; (d) σ^{-1}; (e) τ^{-1}

Propriedades de funções

3.36 Prove: Suponha que $f: A \to B$ e $g: B \to A$ satisfazem $g \circ f = 1_A$. Então f é injetora e g é sobrejetora.

3.37 Prove o Teorema 3.1: Uma função $f: A \to B$ é inversível se, e somente se, f é injetora e sobrejetora.

3.38 Demonstre. Suponha que $f: A \to B$ é inversível com função inversa $f^{-1}: B \to A$. Então, $f^{-1} \circ f = 1_A$ e $f \circ f^{-1} = 1_B$.

3.39 Suponha que $f: A \to B$ é injetora e que $g: A \to B$ é sobrejetora. Seja x um subconjunto de A.

(a) Mostre que $f|_x$, a restrição de f a x, é injetora.

(b) Mostre que $g|_x$ não precisa ser sobrejetora.

3.40 Para cada $n \in \mathbf{N}$, considere o intervalo aberto $A_n = (0, 1/n) = \{x \mid 0 < x < 1/n\}$. Encontre.

(a) $A_2 \cup A_8$; (c) $\cup(A_i : i \in J)$; (e) $\cup(A_i : i \in K)$;

(b) $A_3 \cap A_7$; (d) $\cap(A_i : i \in J)$; (f) $\cap(A_i : i \in K)$;

onde J é um subconjunto finito de $\mathbf{N}$ e $\mathbf{K}$ é um subconjunto infinito de $\mathbf{N}$

3.41 Para cada $n \in N$, faça $D_n = \{n, 2n, 3n, \ldots\} = \{$múltiplos de $n\}$.

(a) Encontre: (i) $D_2 \cap D_7$; (ii) $D_6 \cap D_8$; (iii) $D_3 \cap D_{12}$; (iv) $D_3 \cup D_{12}$.

(b) Prove que $\cap(D_i : i \in K) = \emptyset$, onde K é um subconjunto infinito de $\mathbf{N}$.

3.42 Considere uma classe indexada de conjuntos $\{A_i : i \in I\}$, um conjunto $\mathbf{B}$ e um índice i_0 em I.

Prove: (a) $B \cap (\cup_i A_i) = \cup_i (B \cap A_i)$; (b) $\cap (A_i \mid i \in I) \subseteq A_{i0} \subseteq \cup(A_i \mid i \in I)$.

Números cardinais

3.43 Encontre o número cardinal de cada conjunto. (a) $\{x : x$ é uma letra em "BASEBALL"$\}$, (b) O conjunto potência de $A = \{a, b, c, d, e\}$, (c) $\{x \mid x^2 = 9, 2x = 8\}$

3.44 Determine o número cardinal de.

(a) todas as funções de $A = \{a, b, c, d\}$ em $B = \{1, 2, 3, 4, 5\}$;

(b) todas as funções de P em Q, onde $|P| = r$ e $|Q| = s$;

(c) todas as relações sobre $A = \{a, b, c, d\}$.

(d) todas as relações sobre P, onde $|P| = r$.

3.45 Demonstre:

(a) Todo conjunto infinito A contém um subconjunto D enumerável.

(b) Cada subconjunto de um conjunto enumerável é finito ou enumerável.

(c) Se A e B são enumeráveis, então $A \times B$ é enumerável.

(d) O conjunto **Q** dos números racionais é enumerável.

3.46 Prove: (a) $|A \times B| = |B \times A|$, (b) Se $A \subset B$, então $|A| \leq |B|$, (c) Se $|A| = |B|$, então $|P(A)| = |P(B)|$

Funções especiais

3.47 Encontre: (a) $\lfloor 13{,}2 \rfloor$, $\lfloor -0{,}17 \rfloor$, $\lfloor 34 \rfloor$; (b) $\lceil 13{,}2 \rceil$, $\lceil -0{,}17 \rceil$, $\lceil 34 \rceil$.

3.48 Determine:

(a) 29 (mod 6); (c) 5 (mod 12); (e) −555 (mod 11),

(b) 200 (mod 20); (d) −347 (mod 6)

3.49 Encontre: (a) $3! + 4!$; (b) $3!(3! + 2!)$; (c) $6!/5!$; (d) $30!/28!$

3.50 Calcule: (a) $\log_2 16$; (b) $\log_3 27$; (c) $\log_{10} 0{,}01$.

Problemas variados

3.51 Seja n um inteiro. Encontre $L(25)$ e descreva o que a função L faz, sendo que L é definida por:

$$L(n) = \begin{cases} 0 & \text{se } n = 1 \\ L(\lfloor n/2 \rfloor) + 1 & \text{se } n > 1 \end{cases}$$

3.52 Sejam a e b inteiros. Encontre $Q(2, 7)$, $Q(5, 3)$ e $Q(15, 2)$, onde $Q(a, b)$ é definida por:

$$Q(a, b) = \begin{cases} 5 & \text{se } a < b \\ Q(a - b, b + 2) + a & \text{se } a \geq b \end{cases}$$

3.53 Prove: O conjunto P de todos os polinômios $p(x) = a_0 + a_1x + \cdots + a_m x^m$ com coeficientes inteiros (ou seja, onde $a_0, a_1, \ldots, a_m$ são inteiros) é enumerável.

Respostas dos Problemas Complementares

3.27 (a) Sim, (b) Não; (c) Sim; (d) Não.

3.28 (a) $\{(1, 1), (2, 4), (3, 3), (4, 3)\}$

(b) $\{(1, 1), (2, 2), (3, 1), (4, 1)\}$

(c) $\{(1, 4), (2, 3), (3, 3), (4, 4)\}$

3.29 $\{(a, 4), (b, 6), (c, 4)\}$

3.30 (a) Não; (b) Sim, (c) Não; (d) Sim.

3.31 (a) f, h; (b) f, h, (c) f, h; (d) g.

3.32 (a) f, g; (b) h; (c) Nenhuma; (d) Nenhuma; (e) {todos os números primos}

3.33 (a) g, k; (b) f, g, h; (c) g, (d) Nenhuma.

3.34 $f^{-1}(x) = (x + 7)/3$

3.35 (a) 425631; (b) 416253; (c) 534261, (d) 415623, (e) 453261

3.40 (a) A_2, (b) A_7, (c) A_r, onde r é o menor inteiro em J; (d) A_s, onde s é o maior inteiro em J; (e) A_r, onde r é o menor inteiro em K, (f) $\emptyset$.

3.41 (i) D_{14}; (ii) D_{24}; (iii) D_{12}; (iv) D_3.

3.43 (a) 5; (b) $2^5 = 32$; (c) 0

3.44 (a) $5^4 = 625$; (b) s^r, (c) $2^{16} = 65\,536$; (d) 2.

3.47 (a) 13, -1, 34; (b) 14, 0, 34

3.48 (a) 5; (b) 0; (c) 2; (d) $6 - 5 = 1$; (e) $11 - 5 = 6$.

3.49 (a) 30; (b) 48, (c) 6; (d) 870.

3.50 (a) 4; (b) 3; (c) -2.

3.51 $L(25) = 4$. Cada vez que n é dividido por 2, o valor de L é aumentado por 1. Logo, L é o maior inteiro tal que $2^L < N$. Assim, $L(n) = \lfloor \log_2 n \rfloor$.

3.52 $Q(2, 7) = 5$, $Q(5, 3) = 10$, $Q(15, 2) = 42$.

3.53 Sugestão: Faça P_k o conjunto de polinômios $p(x)$ tais que $m \leq k$, sendo cada $a_i \leq k$. P_k é finito e $P = \cup_k P_k$.

Lógica e Cálculo Proposicional

4.1 INTRODUÇÃO

Muitos algoritmos e demonstrações usam expressões lógicas como:

"SE p ENTÃO q" ou "SE p_1 e p_2, ENTÃO q_1 OU q_2"

Logo, é necessário conhecer os casos nos quais essas expressões são VERDADEIRAS ou FALSAS, ou seja, saber o "valor verdade" de tais expressões. Discutimos essas questões neste capítulo.†

Também investigamos o valor verdade de afirmações quantificadas, as quais são expressões que empregam os quantificadores lógicos "para todo" e "existe".‡

4.2 PROPOSIÇÕES E SENTENÇAS COMPOSTAS

Uma *proposição* (ou *sentença*) é uma afirmação declarativa que é verdadeira ou falsa, mas não ambas. Considere, por exemplo, os seis itens a seguir:

(i) Gelo flutua na água. (iii) $2 + 2 = 4$ (v) Aonde você está indo?
(ii) A China é na Europa. (iv) $2 + 2 = 5$ (vi) Faça seu tema de casa.

Os quatro primeiros são proposições. Os dois últimos não. Além disso, (i) e (iii) são verdadeiras, mas (ii) e (iv) são falsas.

Proposições compostas

Muitas proposições são *compostas*, isto é, formadas por *subproposições* e vários conectivos discutidos a seguir. Tais sentanças são chamadas de *proposições compostas*. Uma proposição é denominada *primitiva* se não puder ser decomposta em proposições mais simples, ou seja, se não for composta.

Por exemplo, as proposições acima, de (i) a (iv), são primitivas. Por outro lado, as duas proposições a seguir são compostas:

"Rosas são vermelhas e violetas são azuis." e "John é esperto ou ele estuda todas as noites."

† N. de T. É importante observar que os autores estão seguindo uma abordagem meramente intuitiva para o cálculo proposicional clássico. Do ponto de vista da lógica matemática, o objetivo do cálculo proposicional não é estabelecer o "valor verdade" de expressões.

‡ N. de T. Normalmente o estudo de quantificadores se faz no cálculo de predicados de primeira ordem e não no cálculo proposicional.

> A propriedade fundamental de uma proposição composta é que seu valor verdade é completamente determinado pelos valores verdade de suas subproposições, junto com a maneira como elas são conectadas para formar as proposições compostas. A seção a seguir explora alguns desses conectivos.

4.3 OPERAÇÕES LÓGICAS BÁSICAS

Esta seção discute as três operações lógicas básicas de conjunção, disjunção e negação, as quais correspondem, respectivamente, às palavras "e", "ou" e "não".

Conjunção, $p \wedge q$

Quaisquer duas proposições podem ser combinadas pela palavra "e" para formar uma proposição composta chamada de *conjunção* das proposições originais. Simbolicamente,

$$p \wedge q$$

que se lê "p e q", denota a conjunção de p e q. Como $p \wedge q$ é uma proposição, ela tem um valor verdade que depende apenas dos valores verdade de p e q. Especificamente:

Definição 4.1: Se p e q são verdadeiras, então $p \wedge q$ é verdadeira; caso contrário, $p \wedge q$ é falsa.

O valor verdade de $p \wedge q$ pode ser definido equivalentemente pela tabela na Fig. 4-1(a). Aqui a primeira linha é uma maneira abreviada de dizer que se p é verdadeira e q é verdadeira, então $p \wedge q$ é verdadeira. A segunda linha diz que se p é verdadeira e q é falsa, então $p \wedge q$ é falsa. E assim por diante. Observe que há quatro linhas correspondentes às quatro possíveis combinações de V e F para as duas subproposições p e q. Note que $p \wedge q$ é verdadeira apenas quando p e q são ambas verdadeiras.

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

(a) p e q

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

(b) p ou q

p	$\neg p$
V	F
F	V

(c) "não p"

Figura 4-1

Exemplo 4.1 Considere as quatro proposições a seguir:

(i) Gelo flutua na água e 2 + 2 = 4. (iii) China é na Europa e 2 + 2 = 4.
(ii) Gelo flutua na água e 2 + 2 = 5. (iv) China é na Europa e 2 + 2 = 5.

Apenas a primeira é verdadeira. As outras são falsas, pois pelo menos uma de suas subproposições é falsa.

Disjunção, $p \vee q$

Duas proposições quaisquer podem ser combinadas pela palavra "ou" para formar uma proposição composta chamada de *disjunção* das proposições originais. Simbolicamente,

$$p \vee q$$

que se lê "p ou q", denota a disjunção de p e q. O valor verdade de $p \vee q$ depende apenas dos valores verdade de p e q como se segue.

Definição 4.2: Se p e q são falsas, então $p \vee q$ é falsa; caso contrário, $p \vee q$ é verdadeira.

O valor verdade de $p \vee q$ pode ser definido equivalentemente pela tabela na Fig. 4-1(b). Observe que $p \vee q$ é falsa apenas no quarto caso, quando p e q são ambas falsas.

Exemplo 4.2 Considere as quatro sentenças a seguir:

(i) Gelo flutua na água ou $2 + 2 = 4$. (iii) China é na Europa ou $2 + 2 = 4$.
(ii) Gelo flutua na água ou $2 + 2 = 5$. (iv) China é na Europa ou $2 + 2 = 5$.

Apenas a última sentença (iv) é falsa. As outras são verdadeiras, uma vez que pelo menos uma de suas subsentenças é verdadeira.

Observação: A palavra "ou" é comumente usada de duas maneiras distintas em português. Às vezes, é empregada no sentido de "p ou q, ou ambas", ou seja, pelo menos uma das duas alternativas acontece; e, às vezes, é usada no sentido de "p ou q, mas não ambas", isto é, somente uma das alternativas ocorre. Por exemplo, a afirmação "Ele irá para Harvard ou Yale" utiliza "ou" no último sentido, chamado eventualmente de *disjunção exclusiva*. A menos que seja estabelecido o contrário, "ou" deve ser empregado no primeiro sentido. Essa discussão aponta para a precisão conquistada em nossa linguagem simbólica. $p \vee q$ é definida por sua tabela verdade e *sempre* significa "p e/ou q".

Negação, $\neg p$

Dada qualquer sentença p, outra sentença, chamada de *negação* de p, pode ser formada escrevendo-se "Não é verdade que . . ." ou "É falso que . . ." antes de p ou, se possível, inserindo em p a palavra "não". Simbolicamente, a negação de p, que se lê "não p", é denotada por

$$\neg p$$

O valor verdade de $\neg p$ depende do valor verdade de p como se segue:

Definição 4.3: Se p é verdadeira, então $\neg p$ é falsa, e se p é falsa, então $\neg p$ é verdadeira.

O valor verdade de $\neg p$ pode ser definido equivalentemente pela tabela da Fig. 4-1(c). Assim, o valor verdade da negação de p é sempre o oposto do valor verdade de p.

Exemplo 4.3 Considere as seis sentenças a seguir:

(a_1) Gelo flutua na água. (a_2) É falso que gelo flutua na água. (a_3) Gelo não flutua na água.
(b_1) $2 + 2 = 5$ (b_2) É falso que $2 + 2 = 5$. (b_3) $2 + 2 \neq 5$

Então, tanto (a_2) quanto (a_3) são a negação de (a_1); e tanto (b_2) quanto (b_3) são a negação de (b_1). Como (a_1) é verdadeira, (a_2) e (a_3) são falsas; e como (b_1) é falsa, (b_2) e (b_3) são verdadeiras.

Observação: A notação lógica para os conectivos "e", "ou" e "não" não é completamente padronizada. Por exemplo, alguns textos usam:

$p \,\&\, q$, $p \cdot q$ ou pq para $p \wedge q$
$p + q$ para $p \vee q$
p', $\bar{p}$ ou $\sim p$ para $\neg p$

4.4 PROPOSIÇÕES E TABELAS VERDADE

Seja $P(p, q, \ldots)$ uma expressão construída a partir de variáveis lógicas $p, q, \ldots$, que assumem o valor VERDADEIRO (V) OU FALSO (F), e a partir dos conectivos lógicos $\wedge$, $\vee$ e $\neg$ (bem como outros discutidos adiante). Tal expressão é chamada de *proposição*.

A principal propriedade de uma proposição $P(p, q, \ldots)$ é que seu valor verdade depende exclusivamente dos valores verdade de suas variáveis, ou seja, o valor verdade de uma proposição é determinado, uma vez que o valor

verdade de cada uma de suas variáveis seja conhecido. Uma maneira concisa e simples para mostrar essa relação é por meio de uma *tabela verdade*. Descrevemos abaixo um modo de obter tal tabela verdade.

Considere, por exemplo, a proposição $\neg(p \wedge \neg q)$. A Fig. 4-2(a) indica como a tabela verdade de $\neg(p \wedge \neg q)$ é construída. Observe que as primeiras colunas da tabela são para as variáveis p, q, e que há linhas suficientes para permitir todas as possíveis combinações de V e F para essas *variáveis*. (Para duas variáveis, como acima, quatro linhas são necessárias, para três variáveis, oito linhas são necessárias, e, no caso geral, para n variáveis, 2^n linhas são necessárias.) Existe, assim, uma coluna para cada estágio "elementar" da construção da proposição, sendo que o valor verdade em cada passo é determinado a partir dos estágios anteriores, pela definição dos conectivos $\wedge$, $\vee$ e $\neg$. Finalmente, obtemos o valor verdade da proposição, o qual aparece na última coluna.

A tabela verdade finalizada da proposição $\neg(p \wedge \neg q)$ é mostrada na Fig. 4-2(b). Ela consiste precisamente nas colunas da Fig. 4-2(a) que aparecem sob as variáveis e sob a proposição; as outras colunas foram meramente usadas na construção da tabela verdade.

p	q	$\neg q$	$p \wedge \neg q$	$\neg(p \wedge \neg q)$
V	V	F	F	V
V	F	V	V	F
F	V	F	F	V
F	F	V	F	V

(a)

p	q	$\neg(p \wedge \neg q)$
V	V	V
V	F	F
F	V	V
F	F	V

(b)

Figura 4-2

Observação: Para evitar um número excessivo de parênteses, às vezes adotamos uma ordem de precedência para os conectivos lógicos. Especificamente,

$$\neg \text{ precede } \wedge, \text{ o qual tem precedência sobre } \vee$$

Por exemplo, $\neg p \wedge q$ significa $(\neg p) \wedge q$ e não $\neg(p \wedge q)$.

Método alternativo para construir uma tabela verdade

Outra maneira para construir a tabela verdade para $\neg(p \wedge \neg q)$ é a seguinte:

(a) Primeiro, construímos a tabela verdade mostrada na Fig. 4-3. Ou seja, primeiro listamos todas as variáveis e as combinações de seus valores verdade. Há também uma linha final rotulada "passo". Em seguida, a proposição é escrita na linha do topo e à direita de suas variáveis, com espaço suficiente de modo a existir uma coluna sob cada variável e sob cada operação lógica na proposição. Por último, (Passo 1), os valores verdade das variáveis são colocados na tabela sob as variáveis na proposição.

(b) Agora valores verdade adicionais são colocados na tabela verdade, coluna por coluna, sob cada operação lógica, como mostrado na Fig. 4-4. Também indicamos o passo no qual cada coluna de valores verdade é colocado na tabela.

A tabela verdade da proposição, portanto, consiste nas colunas originais sob as variáveis e do último passo, ou seja, a última coluna é colocada dentro da tabela.

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V			V
V	F		V			F
F	V		F			V
F	F		F			F
Passo						

Figura 4-3

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V		F	V
V	F		V		V	F
F	V		F		F	V
F	F		F		V	F
Passo			1		2	1

(a)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V	F	F	V
V	F		V	V	V	F
F	V		F	F	F	V
F	F		F	F	V	F
Passo				3	2	1

(b)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V	V	V	F	F	V
F	V	F	V	V	V	F
F	F	V	F	F	F	V
F	F	V	F	F	V	F
Passo		4	1	3	2	1

(c)

Figura 4-4

4.5 TAUTOLOGIAS E CONTRADIÇÕES

Algumas proposições $P(p, q, \ldots)$ contêm apenas V na última coluna de suas tabelas verdade ou, em outras palavras, são verdadeiras para quaisquer valores verdade de suas variáveis. Tais proposições são chamadas de *tautologias*. Analogamente, uma proposição $P(p, q, \ldots)$ é dita uma *contradição* se tiver apenas F na última coluna de sua tabela verdade ou, em outras palavras, se for falsa para quaisquer valores verdade de suas variáveis. Por exemplo, a proposição "p ou não p", isto é, $p \vee \neg p$, é uma tautologia, e a proposição "p e não p", isto é, $p \wedge \neg p$, é uma contradição. Isso é verificado, examinando suas tabelas verdade na Fig. 4-5. (As tabelas verdade têm somente duas linhas, uma vez que cada proposição conta apenas com uma variável p.)

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

(a) $p \vee \neg p$

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

(b) $p \wedge \neg p$

Figura 4-5

Observe que a negação de uma tautologia é uma contradição, pois é sempre falsa. E a negação de uma contradição é uma tautologia, uma vez que é sempre verdadeira.

Agora seja $P(p, q, \ldots)$ uma tautologia, e sejam $P_1(p, q, \ldots)$, $P_2(p, q, \ldots)$, ... proposições quaisquer. Como $P(p, q, \ldots)$ não depende dos valores verdade em particular de suas variáveis $p, q, \ldots$, podemos substituir P_1 por p, P_2 por $q, \ldots$ na tautologia $P(p, q, \ldots)$ e ainda teremos uma tautologia. Em outros termos,

Teorema 4.1 (Princípio de Substituição): Se $P(p, q, \ldots)$ é uma tautologia, então $P(P_1, P_2, \ldots)$ é uma tautologia para quaisquer proposições $P_1, P_2, \ldots$.

4.6 EQUIVALÊNCIA LÓGICA

Duas proposições $P(p, q, \ldots)$ e $Q(p, q, \ldots)$ são *logicamente equivalentes* ou, simplesmente, *equivalentes* ou *iguais*, e se escreve

$$P(p, q, \ldots) \equiv Q(p, q, \ldots)$$

se tiverem tabelas verdade idênticas. Considere, por exemplo, as tabelas verdade de $\neg(p \wedge q)$ e $\neg p \vee \neg q$ que aparecem na Fig. 4-6. Observe que ambas as tabelas verdade são a mesma, isto é, as duas proposições são falsas no primeiro caso e verdadeiras nos outros três casos. Consequentemente, podemos escrever

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

Em outras palavras, as proposições são logicamente equivalentes.

Observação: Sejam p a sentença "Rosas são vermelhas" e q a sentença "Violetas são azuis". Seja S a declaração:

"Não é verdade que rosas são vermelhas e violetas são azuis."

Então S pode ser escrita na forma $\neg(p \wedge q)$. Contudo, como observado acima, $\neg(p \wedge q) \equiv \neg p \vee \neg q$. Consequentemente, S tem o mesmo significado da declaração:

"Rosas não são vermelhas ou violetas não são azuis."

p	q	$p \wedge q$	$\neg(p \wedge q)$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

(a) $\neg(p \wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	F	F	F
V	F	F	V	V
F	V	V	F	V
F	F	V	V	V

(b) $\neg p \vee \neg q$

Figura 4-6

4.7 ÁLGEBRA DE PROPOSIÇÕES

Proposições satisfazem várias leis que são listadas na Tabela 4-1. (Nessa tabela, V e F são restritos aos valores verdade "Verdadeiro" e "Falso", respectivamente.) Estabelecemos esse resultado formalmente.

Teorema 4.2: Proposições satisfazem as leis da Tabela 4-1.

(Observe a semelhança entre a Tabela 4-1 e a Tabela 1-1 sobre conjuntos.)

Tabela 4-1 Leis da álgebra de proposições

Idempotência	(1a) $p \vee p \equiv p$	(1b) $p \wedge p \equiv p$
Associatividade	(2a) $(p \vee q) \vee r \equiv p \vee (q \vee r)$	(2b) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Comutatividade	(3a) $p \vee q \equiv q \vee p$	(3b) $p \wedge q \equiv q \wedge p$
Distributividade	(4a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	(4b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Identidade	(5a) $p \vee F \equiv p$	(5b) $p \wedge V \equiv p$
	(6a) $p \vee V \equiv V$	(6b) $p \wedge F \equiv F$
Involução	(7) $\neg\neg p \equiv p$	
Complementaridade	(8a) $p \vee \neg p \equiv V$	(8b) $p \wedge \neg p \equiv V$
	(9a) $\neg V \equiv F$	(9b) $\neg F \equiv V$
Leis de DeMorgan	(10a) $\neg(p \vee q) \equiv \neg p \wedge \neg q$	(10b) $\neg(p \wedge q) \equiv \neg p \vee \neg q$

4.8 SENTENÇAS CONDICIONAIS E BICONDICIONAIS

Muitas sentenças, especialmente em matemática, são da forma "Se p então q". Tais sentenças são chamadas de *condicionais* e são denotadas por

$$p \rightarrow q$$

A condicional $p \rightarrow q$ é frequentemente lida como "p implica q" ou "p somente se q".

Outra sentença comum é da forma "p se, e somente se, q". Tais sentenças são conhecidas como *bicondicionais* e são denotadas por

$$p \leftrightarrow q$$

Os valores verdade de $p \rightarrow q$ e $p \leftrightarrow q$ são definidos pelas tabelas na Fig. 4-7(a) e (b). Note que:

(a) A condicional $p \rightarrow q$ é falsa apenas quando a primeira parte p é verdadeira e a segunda parte q é falsa. Logo, quando p é falsa, a condicional $p \rightarrow q$ é verdadeira, independentemente do valor verdade de q.

(b) A bicondicional $p \leftrightarrow q$ é verdadeira sempre que p e q têm os mesmos valores verdade e falsa nos demais casos.

A tabela verdade de $\neg p \wedge q$ aparece na Fig. 4-7(c). Observe que a tabela verdade de $\neg p \vee q$ e $p \rightarrow q$ são idênticas, ou seja, são ambas falsas apenas no segundo caso. Consequentemente, $p \rightarrow q$ é logicamente equivalente a $\neg p \vee q$; ou seja,

$$p \rightarrow q \equiv \neg p \vee q$$

Em outras palavras, a sentença condicional "Se p então q" é logicamente equivalente à sentença "Não p ou q", a qual envolve apenas os conectivos $\vee$ e $\neg$ e, assim, já faz parte de nossa linguagem. Podemos considerar $p \rightarrow q$ como uma abreviação para uma sentença recorrente.

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

(a) $p \rightarrow q$

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

(b) $p \leftrightarrow q$

p	q	$\neg p$	$\neg p \vee q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

(c) $\neg p \vee q$

Figura 4-7

4.9 ARGUMENTOS

Um ***argumento*** (ou ***inferência***) é uma afirmação na qual um dado conjunto de proposições $P_1, P_2, \ldots, P_n$, chamadas de ***premissas***, implica (tem como consequência) outra proposição Q, chamada de ***conclusão***. Tal argumento é denotado por

$$P_1, P_2, \ldots, P_n \vdash Q$$

A noção de "argumento lógico" ou "argumento válido" é formalizada como se segue:

Definição 4.4: Um argumento $P_1, P_2, \ldots, P_n \vdash Q$ é dito *válido* se Q é verdadeira se todas as premissas $P_1, P_2, \ldots, P_n$ são verdadeiras.

Um argumento que não é válido é chamado de *falácia*.

Exemplo 4.4

(a) O seguinte argumento é válido:

$$p, p \rightarrow q \vdash q \text{ (\textit{Modus Ponens})}$$

A demonstração dessa regra segue da tabela verdade da Fig. 4-7(a). Especificamente, p e $p \rightarrow q$ são simultaneamente verdadeiras apenas no Caso (linha) 1 e, nesse caso, q é verdadeira.

(b) O argumento a seguir é uma falácia:

$$p \rightarrow q, q \vdash p$$

$p \rightarrow q$ e q são ambas verdadeiras no Caso (linha) 3 da tabela verdade da Fig. 4-7(a), mas, nesse caso, p é falsa.

Agora, as proposições $P_1, P_2, \ldots, P_n$ são simultaneamente verdadeiras se, e somente se, a proposição $P_1 \wedge P_2 \wedge \ldots P_n$ é verdadeira. Assim, o argumento $P_1, P_2, \ldots, P_n \vdash Q$ é válido se, e somente se, Q é verdadeira sempre que $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ for verdadeira ou, equivalentemente, se a proposição $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \rightarrow Q$ for uma tautologia. Estabelecemos esse resultado formalmente.

Teorema 4.3: O argumento $P_1, P_2, \ldots, P_n \vdash Q$ é válido se, e somente se, a proposição $(P_1 \wedge P_2 \ldots \wedge P_n) \rightarrow Q$ é uma tautologia.

Aplicamos esse teorema no exemplo a seguir.

Exemplo 4.5 Um princípio fundamental de raciocínio lógico diz.

"Se p implica q e q implica r, então p implica r"

p	q	r	$[(p$	$\rightarrow$	$q)$	$\wedge$	$(q$	$\rightarrow$	$r)]$	$\rightarrow$	$(p$	$\rightarrow$	$r)$
V	V	V	V	V	V	V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V	F	F	V	V	F	F
V	F	V	V	F	F	F	F	V	V	V	V	V	V
V	F	F	V	F	F	F	F	V	F	V	V	F	F
F	V	V	F	V	V	V	V	V	V	V	F	V	V
F	V	F	F	V	V	F	V	F	F	V	F	V	F
F	F	V	F	V	F	V	F	V	V	V	F	V	V
F	F	F	F	V	F	V	F	V	F	V	F	V	F
Passo			1	2	1	3	1	2	1	4	1	2	1

Figura 4-8

Ou seja, o argumento a seguir é válido.

$$p \rightarrow q,\ q \rightarrow r \vdash p \rightarrow r \text{ (\textit{Lei do Silogismo})}$$

Esse fato é verificado pela tabela verdade na Fig. 4-8, a qual mostra que a seguinte proposição é uma tautologia:

$$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$$

De forma equivalente, o argumento é válido, uma vez que as premissas $p \rightarrow q$ e $q \rightarrow r$ são simultaneamente verdadeiras apenas nos Casos (linhas) 1, 5, 7 e 8 e, nesses casos, a conclusão também é verdadeira. (Observe que a tabela verdade demandou $2^3 = 8$ linhas, pois há três variáveis p, q e r.)

Agora aplicamos a teoria acima sobre argumentos envolvendo sentenças específicas. Enfatizamos que a validade de um argumento não depende dos valores verdade nem do conteúdo das sentenças que surgem no argumento, mas da forma particular da inferência. Isso é ilustrado no exemplo a seguir.

Exemplo 4.6 Considere o seguinte argumento:

S_1: Se um homem é solteiro, ele é infeliz.
S_2: Se um homem é infeliz, ele morre cedo.

S: Solteiros morrem cedo. Silogismo (pois somente duas proposições gera uma conclusão)

Aqui a sentença S abaixo da linha denota a conclusão do argumento, e as sentenças S_1 e S_2 acima da linha correspondem às premissas. Afirmamos que o argumento $S_1, S_2, \vdash S$ é válido, pois ele é da forma

$$p \rightarrow q,\ q \rightarrow r \vdash p \rightarrow r$$

onde p é "Ele é solteiro", q é "Ele é infeliz" e r é "Ele morre cedo"; e pelo Exemplo 4.5 essa inferência (Lei do Silogismo) é válida.

4.10 FUNÇÕES PROPOSICIONAIS, QUANTIFICADORES

Seja A um dado conjunto. Uma *função proposicional* (ou *sentença aberta* ou *condição*) definida sobre A é uma expressão

$$p(x)$$

que tem a propriedade de que $p(a)$ é verdadeira ou falsa para cada $a \in A$. Ou seja, $p(x)$ se torna uma sentença (com um valor verdade) sempre que a variável x é substituída por qualquer elemento $a \in A$. O conjunto A é chamado de

domínio de $p(x)$, e o conjunto T_p de todos os elementos de A para os quais $p(a)$ é verdadeira é chamado de *conjunto verdade* de $p(x)$. Em outras palavras,

$$T_p = \{x \mid x \in A, p(x) \text{ é verdadeira}\} \quad \text{ou} \quad T_p = \{x \mid p(x)\}$$

Frequentemente, quando A é algum conjunto de números, a condição $p(x)$ tem a forma de uma equação ou desigualdade envolvendo a variável x.

Exemplo 4.7 Encontre o conjunto verdade para cada função proposicional $p(x)$ definida sobre o conjunto **N** dos inteiros positivos.

(a) Seja $p(x)$ a fórmula "$x + 2 > 7$" Seu conjunto verdade é $\{6, 7, 8, \ldots\}$, consistindo de todos os inteiros maiores do que 5.

(b) Seja $p(x)$ a fórmula "$x + 5 < 3$" Seu conjunto verdade é o conjunto vazio $\varnothing$ Isto é, $p(x)$ não é verdade para qualquer inteiro em **N**.

(c) Seja $p(x)$ a fórmula "$x + 5 > 1$" Seu conjunto verdade é **N** Ou seja, $p(x)$ é verdadeira para todo elemento de **N**

Observação: O exemplo acima mostra que se $p(x)$ é uma função proposicional definida sobre um conjunto A, então $p(x)$ poderia ser verdadeira para todo $x \in A$, para algum (ou alguns) $x \in A$, ou para nenhum $x \in A$ As duas subseções a seguir discutem quantificadores relacionados com tais funções proposicionais.

Quantificador universal

Seja $p(x)$ uma função proposicional definida sobre um conjunto A. Considere a expressão

$$(\forall x \in A)p(x) \quad \text{ou} \quad \forall x\, p(x) \tag{4.1}$$

a qual se lê "Para todo x em A, $p(x)$ é uma sentença verdadeira" ou, simplesmente, "Para todo x, $p(x)$" O símbolo

$$\forall$$

que se lê "para todo" é chamado de *quantificador universal* A sentença (*4.1*) é equivalente à afirmação

$$T_p = \{x \mid x \in A, p(x)\} = A \tag{4.2}$$

ou seja, à afirmação de que o conjunto verdade de $p(x)$ é o conjunto todo A.

A expressão $p(x)$ em si é uma sentença aberta ou condição e, portanto, não tem valor verdade. Contudo, $\forall x\, p(x)$, isto é, $p(x)$ precedida pelo quantificador $\forall$, tem um valor verdade que segue da equivalência entre (*4.1*) e (*4.2*) Especificamente:

Q_1: Se $\{x \mid x \in A, p(x)\} = A$, então $\forall x\, p(x)$ é verdadeira; caso contrário, $\forall x\, p(x)$ é falsa.

Exemplo 4.8

(a) A proposição $(\forall n \in \mathbf{N})(n + 4 > 3)$ é verdadeira, pois $\{n \mid n + 4 > 3\} = \{1, 2, 3, \ldots\} = \mathbf{N}$

(b) A proposição $(\forall n \in \mathbf{N})(n + 2 > 8)$ é falsa, pois $\{n \mid n + 2 > 8\} = \{7, 8, \ldots\} \neq \mathbf{N}$. Não vale para todos os números naturais

(c) O símbolo $\forall$ pode ser usado para definir a interseção de uma coleção indexada $\{A_i \mid i \in I\}$ de conjuntos A_i como se segue:

$$\cap(A_i \mid i \in I) = \{x \mid \forall_i \in I, x \in A_i\}$$

Quantificador existencial

Seja $p(x)$ uma função proposicional definida sobre um conjunto A Considere a expressão

$$(\exists x \in A)p(x) \quad \text{ou} \quad \exists x, p(x) \tag{4.3}$$

que se lê "Existe um x em A tal que $p(x)$ é uma sentença verdadeira" ou, simplesmente, "Para algum x, $p(x)$". O símbolo

$$\exists$$

o qual se lê "existe" ou "para algum" ou "para pelo menos um" é chamado de *quantificador existencial*. A sentença (4.3) é equivalente à sentença

$$T_p = \{x \mid x \in A, p(x)\} \neq \varnothing \tag{4.4}$$

isto é, à afirmação de que o conjunto verdade de $p(x)$ não é vazio. Conseqüentemente, $\exists x\, p(x)$, ou seja, $p(x)$ precedida pelo quantificador $\exists$, tem um valor verdade. Especificamente,

Q_2: Se $\{x \mid p(x)\} \neq \varnothing$, então $\exists x\, p(x)$ é verdadeira; caso contrário, $\exists x\, p(x)$ é falsa.

Exemplo 4.9

(a) A proposição $(\exists n \in N)(n + 4 < 7)$ é verdadeira, pois $\{n \mid n + 4 < 7\} = \{1, 2\} \neq \varnothing$.

(b) A proposição $(\exists n \in N)(n + 6 < 4)$ é falsa, uma vez que $\{n \mid n + 6 < 4\} = \varnothing$.

(c) O símbolo $\exists$ pode ser usado para definir a união de uma coleção indexada $\{A_i \mid i \in I\}$ de conjuntos A_i, como se segue:

$$\cup(A_i \mid i \in I) = \{x \mid \exists i \in I, x \mid \in A_i\}$$

4.11 NEGAÇÃO DE SENTENÇAS QUANTIFICADAS

Considere a sentença. "Todos os bacharéis em matemática são homens". Sua negação se lê:

"Não é o caso de que todos os bacharéis em matemática são homens" ou, equivalentemente, "Existe pelo menos um bacharel em matemática que é mulher (não é homem)"

Simbolicamente, usando M para denotar o conjunto de bacharéis de matemática, a afirmação acima pode ser escrita como

$$\neg(\forall x \in M)(x \text{ é homem}) \equiv (\exists\, x \in M)\ (x \text{ não é homem})$$

ou, quando $p(x)$ denota "x é homem",

$$\neg(\forall x \in M)\ p(x) \equiv (\exists\, x \in M)\ \neg p(x) \quad \text{ou} \quad \neg\forall x p(x) \equiv \exists x \neg p(x)$$

Isso é verdade para qualquer proposição $p(x)$. Ou seja:

Teorema 4.4 (DeMorgan): $\neg(\forall x \in A)p(x) \equiv (\exists\, x \in A)\neg p(x)$.

Em outras palavras, as duas sentenças a seguir são equivalentes:

(1) Não é verdade que para todo $a \in A$, $p(a)$ é verdadeira. (2) Existe um $a \in A$ tal que $p(a)$ é falsa.

Há um teorema análogo para a negação de uma proposição que contém o quantificador existencial.

Teorema 4.5 (DeMorgan): $\neg(\exists x \in A)p(x) \equiv (\forall x \in A)\neg p(x)$

Ou seja, as duas sentenças a seguir são equivalentes:

(1) Não é verdade que para algum $a \in A$, $p(a)$ é verdadeira. (2) Para todo $a \in A$, $p(a)$ é falsa.

Regra para negar uma sentença quantificada
nega o quatificador e conserva a senteça

ou

troca o quantificador e nega a sentença

Exemplo 4.10

(a) As sentenças a seguir são negações uma da outra:

"Para todos os inteiros positivos n temos $n + 2 > 8$"
"Existe um inteiro positivo n tal que $n + 2 \not> 8$"

(b) As sentenças a seguir também são negações uma da outra:

"Existe uma pessoa (viva) com 150 anos de idade"
"Toda pessoa viva não tem 150 anos de idade"

Observação: A expressão $\neg p(x)$ tem o significado óbvio:

"A sentença $\neg p(a)$ é verdadeira quando $p(a)$ é falsa, e vice-versa"

Anteriormente, $\neg$ foi usado como uma operação sobre sentenças, aqui $\neg$ é usado como uma operação sobre funções proposicionais. Analogamente, $p(x) \wedge q(x)$, que se lê "$p(x)$ e $q(x)$", é definida por:

"A sentença $p(a) \wedge q(a)$ é verdadeira quando $p(a)$ e $q(a)$ são verdadeiras"

Analogamente, $p(x) \vee q(x)$, que se lê "$p(x)$ e $q(x)$", é definida por:

"A sentença $p(a) \vee q(a)$ é verdadeira quando $p(a)$ ou $q(a)$ é verdadeira"

Assim, em termos de conjuntos verdade:

(i) $\neg p(x)$ é o complemento de $p(x)$.
(ii) $p(x) \wedge q(x)$ é a interseção entre $p(x)$ e $q(x)$.
(iii) $p(x) \vee q(x)$ é a união de $p(x)$ com $q(x)$.

Podemos também mostrar que as leis para proposições valem igualmente para funções proposicionais. Por exemplo, temos as Leis de DeMorgan:

$$\neg(p(x) \wedge q(x)) \equiv \neg p(x) \vee \neg q(x) \quad \text{e} \quad \neg(p(x) \vee q(x)) \equiv \neg p(x) \wedge \neg q(x)$$

Contraexemplo

O Teorema 4.6 nos diz que para mostrar que uma sentença $\forall x$, $p(x)$ é falsa, é equivalente mostrar que $\exists\, x \neg p(x)$ é verdadeira ou, em outros termos, que existe um elemento x_0 com a propriedade de que $p(x_0)$ é falsa. Tal elemento x_0 é chamado de *contraexemplo* da afirmação $\forall x$, $p(x)$.

Exemplo 4.11

(a) Considere a sentença $\forall x \in \mathbf{R}$, $|x| \neq 0$. Ela é falsa, pois 0 é um contraexemplo, ou seja, $|0| \neq 0$ não é verdadeira.

(b) Considere a sentença $\forall x \in \mathbf{R}$, $x^2 \geq x$. Ela não é verdadeira, uma vez que, por exemplo, $\frac{1}{2}$ é um contraexemplo. Especificamente, $(\frac{1}{2})^2 \geq \frac{1}{2}$ não é verdadeira, isto é, $(\frac{1}{2})^2 < \frac{1}{2}$.

(c) Considere a sentença $\forall x \in \mathbf{N}$, $x^2 \geq x$. Ela é verdadeira, onde $\mathbf{N}$ é o conjunto de inteiros positivos. Em outras palavras, não existe inteiro positivo n para o qual $n^2 < n$.

Funções proposicionais com mais de uma variável

Uma função proposicional (de n variáveis) definida sobre um produto cartesiano $A = A_1 \times \cdots \times A_n$ é uma expressão

$$p(x_1, x_2, \ldots, x_n)$$

que tem a propriedade de que $p(a_1, a_2, \ldots, a_n)$ é verdadeira ou falsa para qualquer n-upla $p(a_1, \ldots, a_n)$ de A. Por exemplo,

$$x + 2y + 3z < 18$$

é uma função proposicional sobre $\mathbf{N}^3 = \mathbf{N} \times \mathbf{N} \times \mathbf{N}$. Tal função proposicional não tem valor verdade. Contudo, temos o que se segue:

Princípio básico: Uma função proposicional precedida por um quantificador para cada variável, por exemplo,

$$\forall x \exists y, p(x, y) \quad \text{ou} \quad \exists x\, \forall y\, \exists z, p(x, y, z)$$

denota uma sentença e tem um valor verdade.

Exemplo 4.12 Seja $B = \{1, 2, 3, \ldots, 9\}$ e considere que $p(x, y)$ denota "$x + y = 10$". Então $p(x, y)$ é uma função proposicional sobre $A = B^2 = B \times B$.

(a) O que se segue é uma sentença, uma vez que há um quantificador para cada variável.

$$\forall x \exists y, p(x, y), \qquad \text{isto é,} \qquad \text{"Para todo } x \text{, existe } y \text{ tal que } x + y = 10\text{"}$$

Essa sentença é verdadeira. Por exemplo, se $x = 1$, faça $y = 9$; se $x = 2$, faça $y = 8$, e assim por diante.

(b) O que se segue também é uma sentença.

$$\exists y \forall x, p(x, y), \qquad \text{isto é,} \qquad \text{"Existe } y \text{ tal que, para todo } x \text{, temos } x + y = 10\text{"}$$

Não existe tal y; logo, essa sentença é falsa.

Observe que a única diferença entre (a) e (b) é a ordem dos quantificadores. Assim, uma ordenação diferente dos quantificadores pode produzir uma sentença diferente. Notamos que, quando traduzimos tais sentenças quantificadas para o português, a expressão "tal que" frequentemente é seguida por "existe".

Negando sentenças quantificadas com mais de uma variável

Sentenças quantificadas com mais de uma variável podem ser negadas aplicando sucessivamente os Teoremas 4.5 e 4.6. Assim, cada $\forall$ é mudado para $\exists$ e cada $\exists$ é mudado para $\forall$, à medida que o símbolo de negação $\neg$ passa pela sentença, da esquerda para a direita. Por exemplo,

$$\neg[\forall x \exists y \exists z, p(x, y, z)] \equiv \exists x \neg[\exists y \exists z, p(x, y, z)] \equiv \neg \exists z \forall y [\exists z, p(x, y, z)$$
$$\equiv \exists x \forall y \forall z, \neg p(x, y, z)$$

Naturalmente, não colocamos todos os passos quando negamos tais sentenças quantificadas.

Exemplo 4.13

(a) Considere a sentença quantificada.

"Todo estudante cursa pelo menos uma disciplina na qual o docente é um professor assistente."

Sua negação é a sentença:

"Existe um estudante tal que, em toda disciplina cursada, o docente não é um professor assistente."

(b) A definição formal de que L é o limite de uma sequência $a_1, a_2, \ldots$ segue abaixo:

$$\forall \in > 0, \exists n_0 \in \mathbf{N}, \forall_n > n_0, \text{ temos } |a_n - L| < \in$$

Assim, L não é o limite da sequência $a_1, a_2, \ldots$ quando:

$$\exists \in > 0, \forall n_0 \in \mathbf{N}, \exists_n > n_0 \text{ tal que } |a_n - L| \geq \in$$

Problemas Resolvidos

Proposições e tabelas verdade

4.1 Seja p a sentença "Está frio" e seja q "Está chovendo". Dê uma sentença verbal que descreva cada uma das sentenças a seguir: (*a*) $\neg p$; (*b*) $p \wedge q$; (*c*) $p \vee q$; (*d*) $q \vee \neg p$.

Em cada caso, traduza $\wedge$, $\vee$ e $\sim$ como "e", "ou" e "É falso que" ou "não", respectivamente, e então simplifique a sentença em português.

(*a*) Não está frio.

(*b*) Está frio e chovendo.

(*c*) Está frio ou está chovendo.

(*d*) Está chovendo ou não está frio.

4.2 Encontre a tabela verdade de $\neg p \wedge q$.

Construa a tabela verdade de $\neg p \wedge q$ como na Fig. 4-9(*a*).

p	q	$\neg p$	$\neg p \wedge q$
V	V	F	F
V	F	F	F
F	V	V	V
F	F	V	F

(*a*) $\neg p \wedge q$

p	q	$p \wedge q$	$\neg(p \wedge q)$	$p \vee \neg(p \wedge q)$
V	V	V	F	V
V	F	F	V	V
F	V	F	V	V
F	F	F	V	V

(*b*) $p \vee \neg(p \wedge q)$

Figura 4-9

4.3 Verifique que a proposição $p \vee \neg(p \wedge q)$ é uma tautologia.

Construa a tabela verdade de $p \vee \neg(p \wedge q)$ como mostrado na Fig. 4-9(*b*). Como o valor verdade de $p \vee \neg(p \wedge q)$ é V para todos os valores de p e q, a proposição é uma tautologia.

4.4 Mostre que as proposições $\neg(p \wedge q)$ e $\neg p \vee \neg q$ são logicamente equivalentes.

Construa as tabelas verdade para $\neg(p \wedge q)$ e $\neg p \vee \neg q$, como na Fig. 4-10. Como as tabelas verdade são as mesmas (ambas as proposições são falsas no primeiro caso e verdadeiras nos outros três casos), as proposições $\neg(p \wedge q)$ e $\neg p \vee \neg q$ são logicamente equivalentes e podemos escrever

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

p	q	$p \wedge q$	$\neg(p \wedge q)$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

(*a*) $\neg(p \wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	F	F	F
V	F	F	V	V
F	V	V	F	V
F	F	V	V	V

(*b*) $\neg p \vee \neg q$

Figura 4-10

4.5 Use as leis da Tabela 4-1 para mostrar que $\neg(p \wedge q) \vee (\neg p \wedge q) \equiv \neg p$.

Sentença		Justificativa
(1) $\neg(p \vee q) \vee (\neg p \wedge q)$	$\equiv (\neg p \wedge \neg q) \vee (\neg p \wedge q)$	Lei de DeMorgan
(2)	$\equiv \neg p \wedge (\neg q \vee q)$	Distributividade
(3)	$\equiv \neg p \wedge T$	Complementar
(4)	$\equiv \neg p$	Identidade

Sentenças condicionais

4.6 Reescreva as sentenças a seguir sem usar a condicional:

(*a*) Se está frio, ele usa um chapéu.

(*b*) Se a produtividade aumenta, então os salários sobem.

Lembre que "Se p então q" é equivalente a "Não p ou q", ou seja, $p \rightarrow q \equiv \neg p \vee q$. Logo,

(*a*) Não está frio ou ele usa um chapéu.

(*b*) A produtividade não aumenta ou os salários sobem.

4.7 Considere a proposição condicional $p \rightarrow q$. As proposições simples $q \rightarrow p$, $\neg p \rightarrow \neg q$ e $\neg q \rightarrow \neg p$ são chamadas, respectivamente, de *recíproca*, *inversa* e *contrapositiva* da condicional $p \rightarrow q$. Quais dessas proposições, se houver alguma, são logicamente equivalentes a $p \rightarrow q$?

Construa as tabelas verdade como na Fig. 4-11. Apenas a contrapositiva $\neg q \rightarrow \neg p$ é logicamente equivalente à proposição condicional original $p \rightarrow q$.

p	q	$\neg p$	$\neg q$	Condicional $p \rightarrow q$	Recíproca $q \rightarrow p$	Inversa $\neg p \rightarrow \neg q$	Contrapositiva $\neg q \rightarrow \neg p$
V	V	F	F	V	V	V	V
V	F	F	V	F	V	V	F
F	V	V	F	V	F	F	V
F	F	V	V	V	V	V	V

Figura 4-11

4.8 Determine a contrapositiva de cada sentença:

(*a*) Se Érico é um poeta, então ele é pobre.

(*b*) Somente se Marcos estudar, ele passará no teste.

(*a*) A contrapositiva de $p \rightarrow q$ é $\neg q \rightarrow \neg p$. Logo, segue a contrapositiva:

Se Érico não é pobre, então ele não é um poeta.

(*b*) A sentença é equivalente a: "Se passar no teste, então ele estudou". Logo, sua contrapositiva é

Se Marcos não estudar, então ele não passará no teste.

4.9 Escreva a negação de cada sentença da maneira mais simples possível.

(*a*) Ela trabalha e não ganhará dinheiro.

(*b*) Ele nada se, e somente se, a água estiver morna.

(*c*) Se neva, então eles não dirigem o carro.

(*a*) Note que $\neg(p \rightarrow q) \equiv p \wedge \neg q$, logo, a negação da sentença é:

Ela trabalha ou ela não ganhará dinheiro.

(*b*) Observe que $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q$; logo, a negação da sentença é qualquer uma das seguintes

Ele nada se, e somente se, a água não estiver morna.

Ele não nada se, e somente se, a água estiver morna.

(*c*) Note que $\neg(p \rightarrow \neg q) \equiv p \wedge \neg\neg q \equiv p \wedge q$. Logo, a negação da sentença é

Neva e eles dirigem o carro.

Argumentos

4.10 Mostre que o seguinte argumento é uma falácia: $p \rightarrow q, \neg p \vdash \neg q$.

Construa a tabela verdade para $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$, como na Fig. 4-12. Como a proposição $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ não é uma tautologia, o argumento é uma falácia. Equivalentemente, o argumento é falacioso, pois na terceira linha da tabela verdade $p \rightarrow q$ e $\neg p$ são verdadeiras, mas $\neg q$ é falsa.

p	q	$p \rightarrow q$	$\neg p$	$(p \rightarrow q) \wedge \neg p$	$\neg q$	$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$
V	V	V	F	F	F	V
V	F	F	F	F	V	V
F	V	V	V	V	F	F
F	F	V	V	V	V	V

Figura 4-12

4.11 Determine a validade do seguinte argumento: $p \rightarrow q, \neg p \vdash \neg p$.

Construa a tabela verdade para $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$, como na Fig. 4-13. Como a proposição $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p)$ é uma tautologia, o argumento é válido.

p	q	$[(p$	$\rightarrow$	$q)$	$\wedge$	$\neg$	$q]$	$\rightarrow$	$\neg$	p
V	V	V	V	V	F	F	V	V	F	V
V	F	V	F	F	F	V	F	V	F	V
F	V	F	V	V	F	F	V	V	V	F
F	F	F	V	F	V	V	F	V	V	F
Passo		1	2	1	3	2	1	4	2	1

Figura 4-13

4.12 Prove que o argumento a seguir é válido: $p \rightarrow \neg q, r \rightarrow q, r \vdash \neg p$

Construa a tabela verdade das premissas e conclusões, como na Fig. 4-14(*a*). Agora, $p \rightarrow \neg q$, $r \rightarrow q$ e r são simultaneamente verdadeiras apenas na quinta linha da tabela, onde $\neg p$ também é verdadeira. Logo, o argumento é válido

	p	q	r	$p \rightarrow \neg q$	$r \rightarrow q$	$\neg p$
1	V	V	V	F	V	F
2	V	V	F	F	V	F
3	V	F	V	V	F	F
4	V	F	F	V	V	F
5	F	V	V	V	V	V
6	F	V	F	V	V	V
7	F	F	V	V	F	V
8	F	F	F	V	V	V

(*a*)

p	q	q	$r \rightarrow q$	p
V	V	F	F	F
V	F	V	V	F
F	V	F	V	V
F	F	V	V	V

(*b*)

Figura 4-14

4.13 Determine a validade do seguinte argumento:

Se 7 é menor do que 4, então 7 não é um número primo.
7 não é menor do que 4.
―――
7 é um número primo.

Primeiro traduza o argumento em forma simbólica. Seja p a sentença "7 é menor do que 4" e q a sentença "7 é um número primo". Então o argumento é da forma

$$p \to \neg q, \neg q \vdash q$$

Agora, construímos uma tabela verdade como mostrado na Fig. 4-14(*b*). O argumento acima é uma falácia, pois, na quarta linha da tabela, as premissas $p \to \neg q$ e $\neg p$ são verdadeiras, mas a conclusão é falsa.

Observação: O fato de que a conclusão do argumento é uma sentença verdadeira mostra-se irrelevante para o fato de que o argumento apresentado é uma falácia.

4.14 Teste a validade do argumento a seguir:

Se dois lados de um triângulo são iguais, então os ângulos opostos são iguais.
Dois lados de um triângulo não são iguais.
―――
Os ângulos opostos não são iguais.

Primeiro traduza o argumento para a forma simbólica $p \to q, \neg p \vdash \neg q$, onde p é "Dois lados de um triângulo são iguais" e q é "Os ângulos opostos são iguais". Pelo Problema 4.10, esse argumento é uma falácia.

Observação: Apesar de a conclusão *seguir* da segunda premissa e dos axiomas da geometria euclidiana, o argumento acima não constitui uma demonstração, pois ele é uma falácia.

Quantificadores e funções proposicionais

4.15 Seja $A = \{1, 2, 3, 4, 5\}$. Determine o valor verdade de cada uma das sentenças a seguir:

(*a*) $(\exists x \in A)(x + 3 = 10)$ (*c*) $(\exists x \in A)(x + 3 < 5)$
(*b*) $(\forall x \in A)(x + 3 < 10)$ (*d*) $(\forall x \in A)(x + 3 \leq 7)$

(*a*) Falsa, pois nenhum número em A é solução para $x + 3 = 10$.

(*b*) Verdadeira, pois todo número em A satisfaz $x + 3 < 10$.

(*c*) Verdadeira, pois se $x_0 = 1$, então $x_0 + 3 < 5$, ou seja, 1 é a solução.

(*d*) Falsa, pois se $x_0 = 5$, então $x_0 + 3$ não é menor ou igual a 7. Em outras palavras, 5 não é uma solução para a condição dada.

4.16 Determine o valor verdade de cada uma das seguintes sentenças, onde $\mathbf{U} = \{1, 2, 3\}$ é o conjunto universo: (*a*) $\exists x \forall y, x^2 < y + 1$; (*b*) $\forall x \exists y, x^2 + y^2 < 12$; (*c*) $\forall x \forall y, x^2 + y^2 < 12$.

(*a*) Verdadeira, pois se $x = 1$, então 1, 2 e 3 são soluções para $1 < y + 1$.

(*b*) Verdadeira. Para cada x_0 faça $y = 1$; então $x_0^2 + 1 < 12$ é uma sentença verdadeira.

(*c*) Falsa, pois se $x_0 = 2$ e $y_0 = 3$, então $x_0^2 + y_0^2 < 12$ não é uma sentença verdadeira.

4.17 Negue cada uma das sentenças a seguir:

$$(a)\ \exists x\, \forall y,\ p(x, y); \quad (b)\ \forall x\, \forall y,\ p(x, y); \quad (c)\ \exists y\, \exists x\, \forall z,\ p(x, y, z).$$

Use $\neg \forall x\, p(x) \equiv \exists x \neg p(x)$ e $\neg \exists x\, p(x) \equiv \forall x \neg p(x)$:

(*a*) $\neg(\exists x \forall y, p(x, y)) \equiv \forall x \exists y \neg p(x, y)$

(*b*) $\neg(\forall x \forall y, p(x, y)) \equiv \exists x \exists y \neg p(x, y)$

(*c*) $\neg(\exists y\, \exists x\, \forall z, p(x, y, z)) \equiv \forall y\, \forall x\, \exists z, \neg p(x, y, z)$

4.18 Seja $p(x)$ a sentença "$x + 2 > 5$". Estabeleça se $p(x)$ é uma função proposicional sobre cada um dos conjuntos a seguir: (*a*) **N**, o conjunto dos inteiros positivos, (*b*) $M = \{-1, -2, -3, \ldots\}$, (*c*) **C**, o conjunto dos números complexos.

(*a*) Sim.

(*b*) Apesar de $p(x)$ ser falsa para todo elemento de M, $p(x)$ ainda é uma função proposicional sobre M.

(*c*) Não. Observe que $2i + 2 > 5$ não tem qualquer significado. Em outras palavras, desigualdades não são definidas para números complexos.

4.19 Negue cada uma das sentenças a seguir: (*a*) Todos os estudantes vivem nos dormitórios. (*b*) Todos os matemáticos são homens. (*c*) Alguns estudantes têm 25 anos ou mais.

Use o Teorema 4.4 para negar os quantificadores.

(*a*) Pelo menos um estudante não vive nos dormitórios. (Alguns estudantes não vivem nos dormitórios.)

(*b*) Pelo menos um matemático é mulher. (Alguns matemáticos são mulheres.)

(*c*) Nenhum dos estudantes tem 25 anos ou mais. (Todos os estudantes têm menos de 25 anos.)

Problemas Complementares

Proposições e tabelas verdade

4.20 Seja p a sentença "Ele é rico" e seja q "Ele é feliz". Escreva cada sentença na forma simbólica usando p e q. Observe que "Ele é pobre" e "Ele é infeliz" são equivalentes a $\neg p$ e $\neg q$, respectivamente.

(a) Se ele é rico, então ele é infeliz. (c) É necessário ser pobre para ser feliz.

(b) Ele não é rico nem feliz. (d) Ser pobre é ser infeliz.

4.21 Encontre a tabela verdade para (a) $p \vee \neg q$; (b) $\neg p \wedge \neg q$.

4.22 Verifique que a proposição $(p \wedge q) \wedge \neg(p \vee q)$ é uma contradição.

Argumentos

4.23 Teste a validade de cada argumento:

(a) Se chover, Érico ficará doente.
Não choveu.
____
Érico não ficou doente.

(b) Se chover, Érico ficará doente.
Érico não ficou doente.
____
Não choveu.

4.24 Teste a validade do seguinte argumento:
Se eu estudar, então não reprovarei em matemática.
Se eu não jogar basquete, então estudarei.
Mas eu reprovei em matemática.
____
Logo, eu devo ter jogado basquete.

Quantificadores

4.25 Seja $A = \{1, 2, \ldots, 9, 10\}$. Considere cada uma das afirmações a seguir. Se for uma sentença, determine seu valor verdade. Se for uma função proposicional, determine seu conjunto verdade.

(a) $(\forall x \in A)(\exists y \in A)(x + y < 14)$ (c) $(\forall x \in A)(\forall y \in A)(x + y < 14)$

(b) $(\forall y \in A)(x + y < 14)$ (d) $(\exists y \in A)(x + y < 14)$

4.26 Negue cada uma das sentenças a seguir:

(a) Se o professor está ausente, então alguns estudantes não completam suas tarefas de casa.

(b) Todos os estudantes completaram suas tarefas de casa, e o professor está presente.

(c) Alguns dos estudantes não completaram suas tarefas de casa ou o professor está ausente.

4.27 Negue cada sentença no Problema 4.15.

4.28 Encontre um contraexemplo para cada sentença, onde U = {3, 5, 7, 9} é o conjunto universo.

(a) $\forall x, x + 3 \geq 7$, (b) $\forall x$, x é ímpar, (c) $\forall x$, x é primo, (d) $\forall x$, $|x| = x$.

Respostas dos Problemas Complementares

4.20 (a) $p \to \neg q$; (b) $\neg p \wedge \neg q$; (c) $q \to \neg p$; (d) $\neg p \to \neg q$

4.21 (a) V, V, F, V; (b) F, F, F, V.

4.22 Construa sua tabela verdade. É uma contradição, uma vez que sua tabela verdade é falsa para todos os valores de p e q

4.23 Primeiro traduza os argumentos para a forma simbólica: "Chover" para p e "Erik ficará doente" para q.

(a) $p \to q, \neg p \vdash \neg q$ (b) $p \to q, \neg q \vdash \neg p$

Pelo Problema 4.10, (a) é uma falácia. Pelo Problema 4.11, (b) é válido.

4.24 Sejam p "Eu estudo", q "Reprovei em matemática" e r "jogar basquete". O argumento tem a forma:

$$p \to \neg q, \neg r \to p, q \vdash r$$

Construa as tabelas verdade como na Fig. 4-15, onde as premissas $p \to \neg q$, $\neg r \to p$ e q são simultaneamente verdadeiras apenas na quinta linha da tabela e, neste caso, a conclusão r também é verdadeira. Logo, o argumento é válido.

p	q	r	$\neg q$	$p \to \neg q$	$\neg r$	$\neg r \to p$
V	V	V	F	F	F	V
V	V	F	F	F	V	V
V	F	V	V	V	F	V
V	F	F	V	V	V	V
F	V	V	F	V	F	V
F	V	F	F	V	V	F
F	F	V	V	V	F	V
F	F	F	V	V	V	F

Figura 4-15

4.25 (a) A afirmação aberta com duas variáveis é precedida por dois quantificadores, logo, é uma sentença. Além disso, a sentença é verdadeira.

(b) A afirmação aberta é precedida por um quantificador, logo, é uma função proposicional da outra variável. Observe que para todo $y \in A$, $x_0 + y < 14$ se, e somente se, $x_0 = 1, 2$ ou 3. Logo, o conjunto verdade é {1, 2, 3}

(c) É uma sentença e é falsa: se $x_0 = 8$ e $y_0 = 9$, então $x_0 + y_0 < 14$ não é verdade.

(d) É uma afirmação aberta em x. O conjunto verdade é o próprio A.

4.26 (a) O professor está ausente e todos os estudantes completaram suas tarefas de casa.

(b) Alguns dos estudantes não completaram suas tarefas de casa ou o professor está ausente.

(c) Todos os estudantes completaram suas tarefas de casa, e o professor está presente.

4.27 (a) $(\forall x \in A)(x + 3 \neq 10)$ (c) $(\forall x \in A)(x + 3 \geq 5)$

(b) $(\exists x \in A)(x + 3 > 10)$ (d) $(\exists x \in A)(x + 3 > 7)$

4.28 (a) Aqui 3 é contraexemplo.

(b) A sentença é verdadeira; logo, não existe contraexemplo.

(c) Aqui 9 é o único contraexemplo.

(d) A sentença é verdadeira; logo, não há contraexemplo.

Técnicas de Contagem

5.1 INTRODUÇÃO

Este capítulo desenvolve algumas técnicas para determinar, sem enumeração direta, o número de resultados possíveis de um evento em particular ou o número de elementos de um conjunto. Tal contagem sofisticada é, às vezes, chamada de *análise combinatória*. Ela inclui o estudo de permutações e combinações.

5.2 PRINCÍPIOS BÁSICOS DE CONTAGEM

Há dois princípios básicos de contagem usados ao longo deste capítulo. O primeiro envolve adição e, o segundo, multiplicação.

Princípio da Regra da Soma:
Suponha que algum evento E possa ocorrer de m maneiras e um segundo evento F possa ocorrer de n maneiras. Suponha também que ambos os eventos não podem acontecer simultaneamente. Então E ou F podem ocorrer de $m + n$ maneiras.

Princípio da Regra do Produto:
Suponha que existe um evento E que possa ocorrer de m maneiras e, independente deste, há um segundo evento F que pode ocorrer de n maneiras. Então, combinações de E e F podem ocorrer de mn maneiras.

Os princípios acima podem ser estendidos para três ou mais eventos. Ou seja, suponha que um evento E_1 possa ocorrer de n_1 maneiras, um segundo evento E_2 possa ocorrer de n_2 maneiras e, seguindo E_2, um terceiro evento E_3 possa ocorrer de n_3 maneiras e assim por diante. Então:

Regra da Soma: Se nenhum par de eventos pode ocorrer ao mesmo tempo, logo um dos eventos pode ocorrer de

$$n_1 + n_2 + n_3 + \cdots \text{ maneiras.}$$

Regra do Produto: Se os eventos ocorrem um após o outro, então todos os eventos podem ocorrer na ordem indicada de:

$$n_1 \cdot n_2 \cdot n_3 \cdot \ldots \text{ maneiras.}$$

Exemplo 5.1 Suponha que uma faculdade tenha três disciplinas diferentes de história, quatro disciplinas diferentes de literatura e duas disciplinas diferentes de sociologia.

(a) O número m de maneiras que um estudante pode escolher uma de cada tipo de disciplina é:

$$m = 3(4)(2) = 24$$

(b) O número n de maneiras que um estudante pode escolher apenas uma disciplina é:

$$n = 3 + 4 + 2 = 9$$

Há uma interpretação conjuntista dos dois princípios recém-vistos. Especificamente, suponha que $n(A)$ denota o número de elementos em um conjunto A. Então:

(1) ***Princípio da Regra da Soma***: Suponha que A e B são conjuntos disjuntos. Logo,

$$n(A \cup B) = n(A) + n(B)$$

(2) ***Princípio da Regra do Produto***: Seja $A \times B$ o produto cartesiano dos conjuntos A e B. Logo,

$$n(A \times B) = n(A) \cdot n(B)$$

5.3 FUNÇÕES MATEMÁTICAS

Discutimos duas funções matemáticas importantes frequentemente empregadas em combinatória.

Função fatorial

O produto dos inteiros positivos de 1 a n, inclusive, é denotado por $n!$ e se lê "n fatorial" ou "fatorial de n". Logo,

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-2)(n-1)n = n(n-1)(n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$$

Consequentemente, $1! = 1$ e $n! = n(n-1)!$. É também conveniente definir $0! = 1$.

Exemplo 5.2

(a) $3! = 3 \cdot 2 \cdot 1 = 6$, $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$, $5! = 5 \cdot 4! = 5(24) = 120$.

(b) $\dfrac{12 \cdot 11 \cdot 10}{3 \cdot 2 \cdot 1} = \dfrac{12 \cdot 11 \cdot 10 \cdot 9!}{3 \cdot 2 \cdot 1 \cdot 9!} = \dfrac{12!}{3!\,9!}$ e, em termos mais gerais,

$$\frac{n(n-1)\cdots(n-r+1)}{r(r-1)\cdots 3 \cdot 2 \cdot 1} = \frac{n(n-1)\cdots(n-r+1)(n-r)!}{r(r-1)\cdots 3 \cdot 2 \cdot 1 \cdot (n-r)!} = \frac{n!}{r!(n-r)!}$$

(c) Para valores grandes de n, usa-se a aproximação de Stirling (onde $e = 2{,}7128\ldots$):

$$n! = \sqrt{2\pi n}\, n^n e^{-n}$$

Coeficientes binomiais

O símbolo $\binom{n}{r}$, que se lê "nCr" ou "combinação de n por r", onde r e n são inteiros positivos com $r \leq n$, é definido como se segue:

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r(r-1)\ldots 3 \cdot 2 \cdot 1} \quad \text{ou, equivalentemente,} \quad \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Observe que $n - (n - r) = r$. Isso nos leva à importante relação a seguir:

Lema 5.1: $\binom{n}{n-r} = \binom{n}{r}$ ou, equivalentemente, $\binom{n}{a} = \binom{n}{b}$, onde $a + b = n$.

Motivados por esse fato, definimos $0! = 1$. Afinal,

$$\binom{n}{0} = \frac{n!}{0!n!} = 1 \quad \text{e} \quad \binom{0}{0} = \frac{0!}{0!0!} = 1$$

Exemplo 5.3

(a) $\binom{8}{2} = \frac{8 \cdot 7}{2 \cdot 1} = 28, \quad \binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2 \cdot 1} = 126, \quad \binom{12}{5} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 792.$

Observe que $\binom{n}{r}$ tem exatamente r fatores tanto no numerador quanto no denominador.

(b) Suponha que queremos computar $\binom{10}{7}$. Haverá sete fatores em ambos numerador e denominador. Contudo, $10 - 7 = 3$. Logo, usamos o Lema 5.1 para calcular:

$$\binom{10}{7} = \binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120$$

Coeficientes binomiais e triângulo de Pascal

Os números $\binom{n}{r}$ são chamados de *coeficientes binomiais*, uma vez que eles aparecem como coeficientes na expansão $(a + b)^n$. Especificamente:

Teorema (Binomial) 5.2: $(a + b)^n = \sum_{k=0}^{n} \binom{n}{r} a^{n-k} b^k$

Os coeficientes das potências sucessivas de $a + b$ podem ser arranjados em uma disposição triangular de números, chamada de triângulo de Pascal, como representado na Fig. 5-1. Os números no triângulo de Pascal têm as seguintes propriedades interessantes:

(i) O primeiro e o último número em cada linha é 1.

(ii) Todos os demais números podem ser obtidos, adicionando os dois números que aparecem acima deles. Por exemplo:

$$10 = 4 + 6, \; 15 = 5 + 10, \; 20 = 10 + 10.$$

Uma vez que esses números são coeficientes binomiais, estabelecemos formalmente a propriedade acima.

$$(a+b)^0 = 1$$
$$(a+b)^1 = a + b$$
$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$
$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$
$$(a+b)^6 = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6$$
$$\dots$$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1

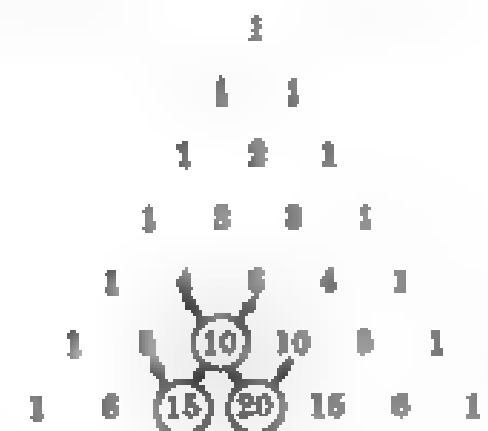



Figura 5-1 Triângulo de Pascal.

Teorema 5.3: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

5.4 PERMUTAÇÕES

Qualquer disposição de um conjunto de n objetos em uma dada ordem é chamada de *permutação* dos objetos (tomados todos de uma vez). Uma disposição de quaisquer $r < n$ desses objetos em uma dada ordem é chamada de "r-permutação" ou "permutação de n objetos tomados r por vez". Considere, por exemplo, o conjunto de letras A, B, C, D. Então:

(i) $BDCA$, $DCBA$ e $ACDB$ são permutações das quatro letras (tomadas todas de uma vez).

(ii) BAD, ACB e DBC são permutações das quatro letras tomadas três por vez.

(iii) AD, BC e CA são permutações das quatro letras tomadas duas por vez.

Geralmente, estamos interessados na quantia de tais permutações sem listá-las.
O número de permutações de n objetos tomados r por vez é denotado por

$$P(n, r) \quad \text{(outros textos podem usar } {}_nP_r,\ P_{n,r} \text{ ou } (n)_r\text{)}.$$

O teorema a seguir se aplica.

Teorema 5.4: $P(n, r) = n(n-1)(n-2)\cdots(n-r+1) = \dfrac{n!}{(n-r)!}$

Enfatizamos que existem r fatores em $n(n-1)(n-2)\cdots(n-r+1)$.

Exemplo 5.4 Encontre o número m de permutações de seis objetos, digamos, A, B, C, D, E, F, tomados três por vez. Em outras palavras, determine a quantia de "palavras de três letras" usando apenas as seis letras dadas sem repetição.

Representemos a palavra genérica de três letras pelas três posições seguintes:

$$___, ___, ___$$

A primeira letra pode ser escolhida de 6 maneiras; seguindo esta, a segunda letra pode ser escolhida de 5 maneiras, e, finalmente, a terceira letra pode escolhida de 4 maneiras. Escrevemos cada número em sua posição apropriada como se segue

$$\underline{6}, \underline{5}, \underline{4}$$

Pela Regra do Produto, há $m = 6 \cdot 5 \cdot 4 = 120$ possíveis palavras de três letras sem repetição, a partir das seis letras. Logo, existem 120 permutações de 6 objetos tomados 3 por vez. Isso está de acordo com a fórmula do Teorema 5.4:

$$P(6, 3) = 6 \cdot 5 \cdot 4 = 120$$

De fato, o Teorema 5.4 é demonstrado da mesma maneira como fizemos neste caso em particular.

Considere agora o caso especial de $P(n, r)$, quando $r = n$. Obtemos o seguinte resultado.

Corolário 5.5: Existem $n!$ permutações de n objetos (tomados todos de uma vez).

Por exemplo, há $3! = 6$ permutações das três letras A, B, C. Elas são

$$ABC, \quad ACB, \quad BAC, \quad BCA, \quad CAB, \quad CBA.$$

Permutações com repetições

Frequentemente, queremos saber o número de permutações de um multiconjunto, ou seja, um conjunto de objetos tais que alguns são repetidos. Denotamos por

$$P(n; n_1, n_2, \ldots, n_r)$$

o número de permutações de n objetos, dos quais n_1 são repetidos, n_2 são repetidos, ..., n_r são repetidos. A fórmula geral é a seguinte:

Teorema 5.6: $P(n; n_1, n_2, \ldots, n_r) = \dfrac{n!}{n_1!\,n_2!\cdots n_r!}$

Indicamos a demonstração do teorema acima com um exemplo específico. Suponha que queremos formar todas as possíveis "palavras" com cinco letras, usando os caracteres da palavra "*BABBY*". Existem $5! = 120$ permutações dos objetos B_1, A, B_2, B_3, Y, onde os três Bs são distinguidos. Observe que as seis permutações a seguir

$$B_1 B_2 B_3 AY,\quad B_2 B_1 B_3 AY,\quad B_3 B_1 B_2 AY,\quad B_1 B_3 B_2 AY,\quad B_2 B_3 B_1 AY,\quad B_3 B_2 B_1 AY$$

produzem a mesma palavra quando os subscritos são removidos. O 6 vem do fato de que há $3! = 3 \cdot 2 \cdot 1 = 6$ maneiras distintas para colocar os três B's nas três primeiras posições da permutação. Isso é verdade para cada conjunto de três posições nas quais os B's podem aparecer. Consequentemente, o número de palavras diferentes de cinco letras que podem ser formadas, usando as letras da palavra "*BABBY*" é:

$$P(5, 3) = \frac{5!}{3!} = 20$$

Exemplo 5.5 Encontre o número m de palavras de sete letras que podem ser formadas, usando as letras da palavra "*BENZENE*".

Buscamos o número de permutações de 7 objetos, dos quais 3 são indistinguíveis (os três E's), e 2 são indistinguíveis (os dois N's). Pelo Teorema 5.6,

$$m = P(7, 3, 2) = \frac{7!}{3!2!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = 420$$

Amostras ordenadas

Muitos problemas se referem à escolha de um elemento a partir de um conjunto S, digamos, com n elementos. Quando escolhemos um elemento após o outro, digamos, r vezes, chamamos a escolha de *amostra ordenada* de tamanho r. Consideramos dois casos.

(1) Amostragem com reposição

Aqui o elemento é devolvido ao conjunto S antes que o próximo objeto seja escolhido. Assim, em cada vez existem n maneiras para escolher um elemento (repetições são permitidas). A Regra do Produto nos diz que o número de tais amostras é:

$$n \cdot n \cdot n \cdots n \cdot n (r \text{ fatores}) = n^r$$

(2) Amostragem sem reposição

Aqui o elemento não é devolvido ao conjunto S antes que o próximo seja escolhido. Logo, não há repetição na amostra ordenada. Tal amostra é simplesmente uma r-permutação. Assim, o número de tais amostras é:

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

Exemplo 5.6 Três cartas são escolhidas uma após a outra em uma baralho de 52 cartas. Encontre o número m de maneiras que isso pode ser feito: (a) com reposição; (b) sem reposição.

(a) Cada carta pode ser escolhida de 52 maneiras. Logo, $m = 52(52)(52) = 140\,608$.

(b) Aqui não há devolução. Portanto, a primeira carta pode ser escolhida de 52 maneiras, a segunda de 51, e a terceira de 50 maneiras. Logo,

$$m = P(52,3) = 52(51)(50) = 132\,600$$

5.5 COMBINAÇÕES

Seja S um conjunto com n elementos. Uma *combinação* desses n elementos tomados r por vez é qualquer seleção de r dos elementos, onde a ordem não interessa. Tal seleção é chamada de *r-combinação*; é simplesmente um subconjunto de S com r elementos. O número de tais combinações é denotado por

$$C(n, r) \qquad \text{(outros textos podem usar } {}_nC_r,\ C_{n,r} \text{ ou } C_r^n\text{).}$$

Antes de apresentarmos a fórmula geral para $C(n, r)$, consideraremos um caso especial.

Exemplo 5.7 Encontre o número de combinações de 4 objetos A, B, C, D, tomados 3 por vez.

Cada combinação de três objetos determina $3! = 6$ permutações dos objetos como se segue.

$$\begin{array}{lllllll}
ABC: & ABC, & ACB, & BAC, & BCA, & CAB, & CBA \\
ABD: & ABD, & ADB, & BAD, & BDA, & DAB, & DBA \\
ACD: & ACD, & ADC, & CAD, & CDA, & DAC, & DCA \\
BCD: & BDC, & BDC, & CBD, & CDB, & DBC, & DCB
\end{array}$$

Assim, o número de combinações multiplicado por 3! nos dá o número de permutações, ou seja,

$$C(4, 3) \cdot 3! = P(4, 3) \quad \text{ou} \quad C(4, 3) = \frac{P(4, 3)}{3!}$$

Mas $P(4, 3) = 4 \cdot 3 \cdot 2 = 24$ e $3! = 6$; logo, $C(4, 3) = 4$, como observado acima.

Como indicado, qualquer combinação de n objetos, tomados r por vez, determina $r!$ permutações dos objetos na combinação; isto é,

$$P(n, r) = r!\, C(n, r)$$

Consequentemente, obtemos a seguinte fórmula para $C(n, r)$, que formalmente estabelecemos como um teorema.

Teorema 5.7: $C(n, r) = \dfrac{P(n, r)}{r!} = \dfrac{n!}{r!(n-r)!}$

Lembre que o coeficiente binomial $\dbinom{n}{r}$ foi definido como $\dfrac{n!}{r!(n-r)!}$, logo,

$$\boxed{C(r, n) = \binom{n}{r}}$$

Devemos usar $C(n, r)$ e $\dbinom{n}{r}$ como sinônimos.

Exemplo 5.8 Um fazendeiro compra 3 vacas, 2 porcos e 4 galinhas de um homem que tem 6 vacas, 5 porcos e 8 galinhas. Encontre o número m de escolhas que o fazendeiro tem.

O fazendeiro pode escolher as vacas de $C(6, 3)$ maneiras, os porcos de $C(5, 2)$ e as galinhas de $C(8, 4)$. Assim, o número m de escolhas é o seguinte:

$$m = \binom{6}{3}\binom{5}{2}\binom{8}{4} = \frac{6 \cdot 5 \cdot 4}{3 \cdot 2 \cdot 1} \cdot \frac{5 \cdot 4}{2 \cdot 1} \cdot \frac{8 \cdot 7 \cdot 6 \cdot 5}{4 \cdot 3 \cdot 2 \cdot 1} = 20 \cdot 10 \cdot 70 = 14\,000$$

5.6 PRINCÍPIO DA CASA DOS POMBOS

Muitos resultados em combinatória derivam da afirmação quase óbvia a seguir

Princípio da Casa dos Pombos: Se n casas são ocupadas por $n + 1$ ou mais pombos, então pelo menos uma casa é ocupada por mais de um pombo.

Esse princípio pode ser aplicado a muitos problemas nos quais queremos mostrar que uma dada situação pode acontecer

Exemplo 5.9

(a) Suponha que um departamento contém 13 professores. Então dois dos professores (pombos) nasceram no mesmo mês (casa)

(b) Encontre o menor número de elementos necessários para tirar do conjunto $S = \{1, 2, 3, \ldots, 9\}$ para ter certeza de que dois dos números somam 10.

Aqui as casas são os cinco conjuntos $\{1, 9\}$, $\{2, 8\}$, $\{3, 7\}$, $\{4, 6\}$ e $\{5\}$. Assim, qualquer escolha de seis elementos (pombos) de S garante que dois dos números somam 10.

O Princípio da Casa dos Pombos é generalizado como se segue.

Princípio generalizado da casa dos pombos: Se n casas são ocupadas por $kn + 1$ ou mais pombos, onde k é um inteiro positivo, então pelo menos uma casa é ocupada por $k + 1$ ou mais pombos.

Exemplo 5.10 Encontre o número mínimo de estudantes em uma turma para ter certeza de que três deles nasceram no mesmo mês.

Aqui $n = 12$ meses são as casas, e $k + 1 = 3$; assim, $k = 2$. Logo, entre $kn + 1 = 25$ estudantes (pombos), três deles nasceram no mesmo mês.

5.7 PRINCÍPIO DE INCLUSÃO-EXCLUSÃO

Sejam A e B conjuntos finitos quaisquer. Lembre do Teorema 1.9, que nos diz.

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Em outras palavras, para encontrar o número $n(A \cup B)$ de elementos na união de A com B, somamos $n(A)$ e $n(B)$ e então subtraímos $n(A \cap B)$; ou seja, "incluímos" $n(A)$ e $n(B)$ e "excluímos" $n(A \cap B)$. Isso segue do fato de que, quando somamos $n(A)$ e $n(B)$, contamos os elementos de $(A \cap B)$ duas vezes.

O princípio acima vale para qualquer número de conjuntos. Primeiro o estabelecemos para três conjuntos.

Teorema 5.8: Para quaisquer conjuntos finitos A, B e C temos.

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Ou seja, "incluímos" $n(A)$, $n(B)$ e $n(C)$, "excluímos" $n(A \cap B)$, $n(A \cap C)$ e $n(B \cap C)$, e finalmente "incluímos" $n(A \cap B \cap C)$.

Exemplo 5.11 Encontre o número de alunos de matemática, em uma faculdade, estudando pelo menos um dos idiomas francês, alemão e russo, dadas as seguintes informações.

65 estudam francês,	20 estudam francês e alemão,	
45 estudam alemão,	25 estudam francês e russo,	8 estudam as três línguas.
42 estudam russo,	15 estudam alemão e russo.	

Queremos encontrar $n(F \cup G \cup R)$, onde F, G e R denotam os conjuntos de alunos estudando francês, alemão e russo, respectivamente.

Pelo Princípio de Inclusão-Exclusão,

$$\begin{aligned} n(F \cup G \cup R) &= n(F) + n(G) + n(R) - n(F \cap G) - n(F \cap R) - n(G \cap R) + n(F \cap G \cap R) \\ &= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100 \end{aligned}$$

Logo, 100 alunos estudam pelo menos uma das três línguas.

Agora, suponha que temos qualquer número finito de conjuntos finitos, digamos, $A_1, A_2, \ldots, A_m$. Seja s_k a soma das cardinalidades

$$n(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k})$$

de todas as possíveis interseções k-uplas dos m conjuntos dados. Então temos o seguinte Princípio de Inclusão--Exclusão generalizado.

Teorema 5.9: $n(A_1 \cup A_2 \cup \cdots \cup A_m) = s_1 - s_2 + s_3 - \cdots + (-1)^{m-1}s_m$.

5.8 DIAGRAMAS EM ÁRVORE

Um *diagrama em árvore* é um dispositivo usado para enumerar todos os possíveis resultados de uma sequência de eventos, onde cada evento pode ocorrer em uma quantia finita de maneiras. A construção de diagramas em árvore é ilustrada no exemplo a seguir.

Exemplo 5.12

(a) Encontre o produto cartesiano $A \times B \times C$, onde $A = \{1, 2\}$, $B = \{a, b, c\}$ e $C = \{x, y\}$

O diagrama em árvore para $A \times B \times C$ aparece na Fig. 5-2(a). Aqui a árvore é construída da esquerda para a direita, e o número de ramos em cada ponto corresponde aos possíveis resultados do próximo evento. Cada ponto terminal (folha) da árvore é rotulado pelo elemento correspondente de $A \times B \times C$. Como observado anteriormente, $A \times B \times C$ tem $n = 2(3)(2) = 12$ elementos.

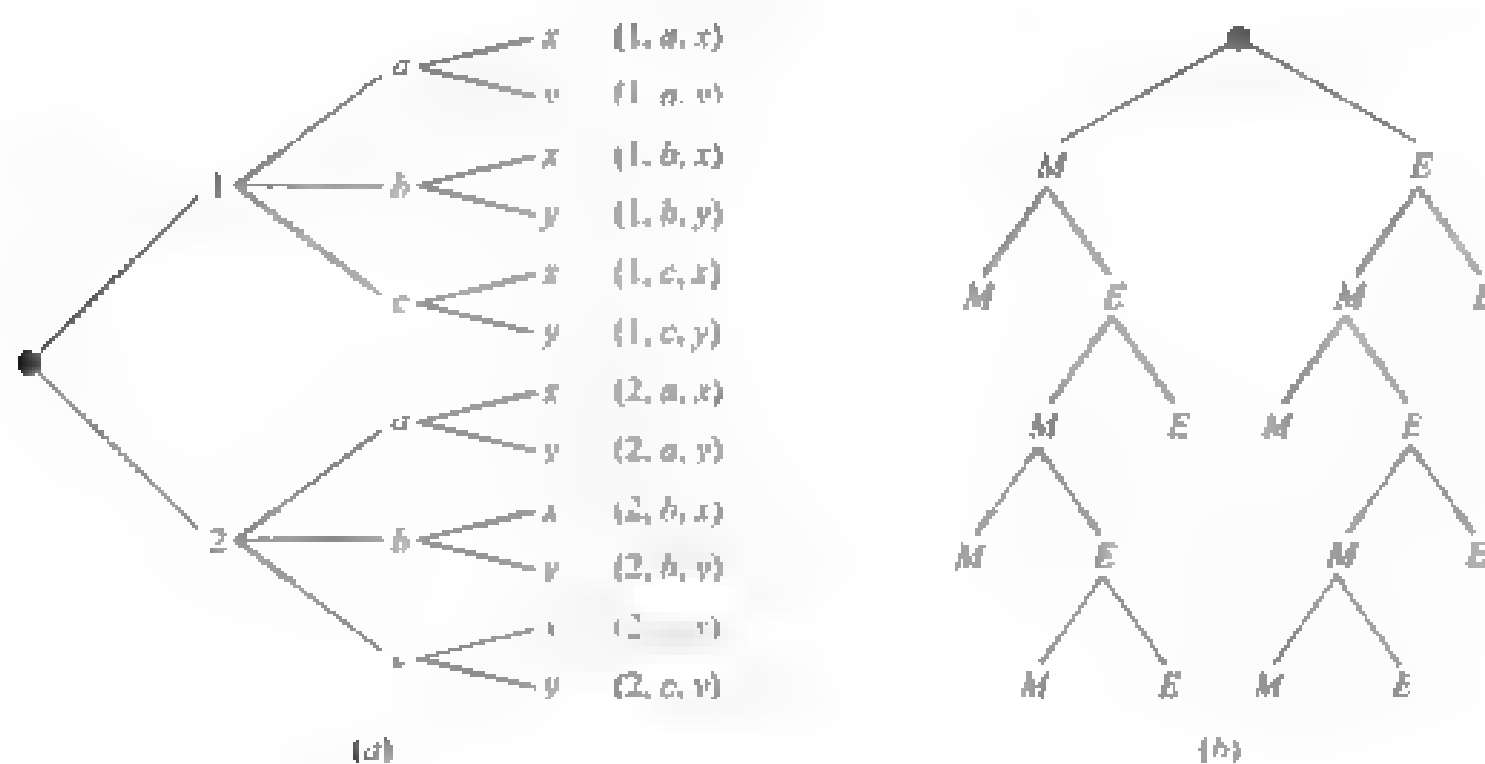



Figura 5-2

(b) Marcos e Érico jogarão em um torneio de tênis. A primeira pessoa que vencer dois jogos seguidos, ou aquele que ganhar um total de três jogos, vence o torneio. Encontre o número de maneiras que o torneio pode desenvolver.

O diagrama em árvore mostrando os possíveis resultados do torneio aparece na Fig. 5-2(b). Aqui a árvore é construída de cima para baixo em vez da esquerda para a direita. (Isto é, a "raiz" está no topo da árvore.) Observe que há 10 pontos terminais, e eles correspondem às dez maneiras a seguir que o torneio pode ocorrer:

$$MM,\ MEMM,\ MEMEM,\ MEMEE,\ MEE,\ EMM,\ EMEMM,\ EMEME,\ EMEE,\ EE$$

O caminho do início (no alto) da árvore até o ponto terminal descreve quem ganha em cada jogo do torneio.

Problemas Resolvidos

Notação fatorial e coeficientes binomiais

5.1 Calcule: (*a*) 4!, 5!; (b) 6!, 7!, 8!, 9!; (c) 50!

(*a*) $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$, $\quad 5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5(24) = 120$.

(*b*) Agora use $(n+1)! = (n+1)n!$.

$$6! = 5(5!) = 6(120) = 720, \qquad 8! = 8(7!) = 8(5040) = 40\,320,$$
$$7! = 7(6!) = 7(720) = 5\,040, \qquad 9! = 9(8!) = 9(40\,320) = 362\,880.$$

(*c*) Como n é muito grande, usamos a aproximação de Stirling: $n! = \sqrt{2\pi n}\, n^n e^{-n}$ (onde $e \approx 2{,}718$). Logo,

$$50! \approx N = \sqrt{100\pi}\, 50^{50} e^{-50}$$

Desenvolvendo N com uma calculadora, obtemos $N = 3{,}04 \times 10^{64}$ (que tem 65 dígitos).

5.2 Calcule: (*a*) $\dfrac{13!}{11!}$; (*b*) $\dfrac{7!}{10!}$.

(*a*) $\dfrac{13!}{11!} = \dfrac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 13 \cdot 12 = 156$.

Alternativamente, isso poderia ser resolvido como se segue:

$$\frac{13!}{11!} = \frac{13 \cdot 12 \cdot 11!}{11!} = 13 \cdot 12 = 156.$$

(*b*) $\dfrac{7!}{10!} = \dfrac{7!}{10 \cdot 9 \cdot 8 \cdot 7!} = \dfrac{1}{10 \cdot 9 \cdot 8} = \dfrac{1}{720}$

5.3 Simplifique: (*a*) $\dfrac{n!}{(n-1)!}$, (*b*) $\dfrac{(n+2)!}{n!}$

(*a*) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = n$; alternativamente, $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n$

(*b*) $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n!}{n!} = (n+2)(n+1) = n^2 + 3n + 2$.

5.4 Calcule: (*a*) $\dbinom{16}{3}$, (*b*) $\dbinom{12}{4}$, (*c*) $\dbinom{8}{5}$

Lembre que existem tantos fatores no numerador quanto no denominador.

(*a*) $\dbinom{16}{3} = \dfrac{16 \cdot 15 \cdot 14}{3 \cdot 2 \cdot 1} = 560$; (*b*) $\dbinom{12}{4} = \dfrac{12 \cdot 11 \cdot 10 \cdot 9}{4 \cdot 3 \cdot 2 \cdot 1} = 495$

(*c*) Como $8 - 5 = 3$, temos $\dbinom{8}{5} = \dbinom{8}{3} = \dfrac{8 \cdot 7 \cdot 6}{3 \cdot 2 \cdot 1} = 56$

5.5 Demonstre: $\dbinom{17}{6} = \dbinom{16}{5} + \dbinom{16}{6}$

Temos $\dbinom{16}{5} + \dbinom{16}{6} = \dfrac{16!}{5!\,11!} + \dfrac{16!}{6!\,10!}$. Multiplique a primeira fração por $\frac{6}{6}$ e a segunda por $\frac{11}{11}$ para obter o mesmo denominador em ambas as frações, e então some.

$$\binom{16}{5} + \binom{16}{6} = \frac{6 \cdot 16!}{6 \cdot 5! \cdot 11!} + \frac{11 \cdot 16!}{6! \cdot 11 \cdot 10!} = \frac{6 \cdot 16!}{6! \cdot 11!} + \frac{11 \cdot 16!}{6! \cdot 11!}$$
$$= \frac{6 \cdot 16! + 11 \cdot 16!}{6! \cdot 11!} = \frac{(6+11) \cdot 16!}{6! \cdot 11!} = \frac{17 \cdot 16!}{6! \cdot 11!} = \frac{17!}{6! \cdot 11!} = \binom{17}{6}$$

5.6 Prove o Teorema 5.3: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

(A técnica nessa demonstração é semelhante àquela do problema anterior.)

Temos $\binom{n}{r-1} + \binom{n}{r} = \frac{n!}{(r-1)!\cdot(n-r+1)!} + \frac{n!}{r!\cdot(n-r)!}$

Para obter o mesmo denominador em ambas as frações, multiplique a primeira fração por $\frac{r}{r}$ e a segunda por $\frac{n-r+1}{n-r+1}$.

Logo,

$$\begin{aligned}
\binom{n}{r-1} + \binom{n}{r} &= \frac{r\cdot n!}{r\cdot(r-1)!\cdot(n-r+1)!} + \frac{(n-r+1)\cdot n!}{r!\cdot(n-r+1)\cdot(n-r)!} \\
&= \frac{r\cdot n!}{r!(n-r+1)!} + \frac{(n-r+1)\cdot n!}{r!(n-r+1)!} \\
&= \frac{r\cdot n! + (n-r+1)\cdot n!}{r!(n-r+1)!} = \frac{[r+(n-r+1)]\cdot n!}{r!(n-r+1)!} \\
&= \frac{(n+1)n!}{r!(n-r+1)!} = \frac{(n+1)!}{r!(n-r+1)!} = \binom{n+1}{r}
\end{aligned}$$

Princípios de contagem

5.7 Suponha que em uma estante tenha 5 textos de história, 3 de sociologia e 4 de psicologia. Encontre o número n de maneiras que um estudante pode escolher:

(a) um dos textos; (b) um texto de cada tipo.

(a) Aqui a Regra da Soma se aplica; logo, $n = 5 + 3 + 6 + 4 = 18$.

(b) Aqui a Regra do Produto se aplica; logo, $n = 5 \cdot 3 \cdot 6 \cdot 4 = 360$.

5.8 Uma turma de história contém 8 homens e 6 mulheres. Encontre o número de maneiras que a turma pode eleger: (a) 1 representante, (b) 2 representantes, um homem e uma mulher; (c) 1 presidente e 1 vice-presidente.

(a) Aqui a Regra da Soma é usada; logo, $n = 8 + 6 = 14$.

(b) Aqui a Regra do Produto é usada; logo, $n = 8 \cdot 6 = 48$

(c) Existem 14 maneiras de eleger o presidente e, então, 13 maneiras de eleger o vice-presidente. Logo, $n = 14 \cdot 13 = 182$.

5.9 Há quatro linhas de ônibus entre A e B, e três entre B e C. Encontre o número m de maneiras que um homem pode viajar de ônibus: (a) de A a C, passando por B; (b) ida e volta de A a C, passando por B; (c) ida e volta de A a C, passando por B, mas sem usar uma linha de ônibus mais de uma vez.

(a) Há 4 maneiras de ir de A a B e 3 maneiras de B a C; logo, $n = 4 \cdot 3 = 12$.

(b) Há 12 maneiras de ir de A a C, passando por B, e 12 maneiras de voltar. Logo, $n = 12 \cdot 12 = 144$

(c) O homem viajará de A a B a C a B a A. Exiba essas letras com flechas de conexão como se segue:

$$A \rightarrow B \rightarrow C \rightarrow B \rightarrow A$$

O homem pode viajar de duas maneiras de A para B e de três de B para C, mas ele só pode viajar de duas maneiras de C para B e de três maneiras de B para A, desde que ele não queira usar a mesma linha de ônibus mais de uma vez. Exiba esses números acima das setas correspondentes, como se segue:

$$A \overset{4}{\rightarrow} B \overset{3}{\rightarrow} C \overset{2}{\rightarrow} B \overset{3}{\rightarrow} A$$

Logo, pela Regra do Produto, $n = 4 \cdot 3 \cdot 2 \cdot 3 = 72$.

Permutações

5.10 Estabeleça a diferença essencial entre permutações e combinações, com exemplos.

A ordem é relevante em permutações, como em palavras, filas e eleições de presidente, vice-presidente e tesoureiro. A ordem é irrelevante em combinações, como em comitês e times (ignorando posições). A regra do produto é geralmente

usada em permutações, uma vez que a escolha para cada uma das posições ordenadas pode ser entendida como uma sequência de eventos.

5.11 Encontre: (*a*) $P(7, 3)$; (*b*) $P(14, 2)$.

Lembre que $P(n, r)$ tem r fatores começando com n.

(*a*) $P(7, 3) = 7 \cdot 6 \cdot 5 = 210$; (*b*) $P(14, 2) = 14 \cdot 13 = 182$.

5.12 Encontre o número m de maneiras que 7 pessoas podem ser dispostas:

(*a*) Em uma fila de cadeiras; (*b*) Em torno de uma mesa redonda.

(*a*) Aqui $m = P(7, 7) = 7!$ maneiras.

(*b*) Uma pessoa pode sentar em qualquer lugar à mesa. As outras seis pessoas podem ser dispostas de 6! maneiras em torno da mesa, ou seja, $m = 6!$.

Esse é um exemplo de *permutação circular*. No caso geral, n objetos podem ser dispostos em um círculo de $(n - 1)!$ maneiras.

5.13 Encontre o número n de permutações distintas que podem ser formadas a partir de todas as letras de cada palavra:

(*a*) THOSE; (*b*) UNUSUAL; (*c*) SOCIOLOGICAL.

Esse problema se refere a permutações com repetições.

(*a*) $n = 5! = 120$, uma vez que há 5 letras e nenhuma repetição.

(*b*) $n = \frac{7!}{3!} = 840$, pois existem 7 letras, das quais 3 são U e nenhuma outra é repetida.

(*c*) $n = \frac{12!}{3!\,2!\,2!\,2!}$, pois há 12 letras, das quais 3 são O, 2 são C, 2 são I e 2 são L. (Deixamos a resposta usando fatoriais, pois o número é muito grande.)

5.14 Uma turma contém 8 estudantes. Encontre o número n de amostras de tamanho 3.

(*a*) Com reposição; (*b*) Sem reposição.

(*a*) Cada estudante na amostra ordenada pode ser escolhido de 8 maneiras; logo, há

$$n = 8 \cdot 8 \cdot 8 = 8^3 = 512 \text{ amostras de tamanho 3 com reposição.}$$

(*b*) O primeiro estudante na amostra pode ser escolhido de 8 maneiras, o segundo de 7, e o último de 6. Assim, há $n = 8 \cdot 7 \cdot 6 = 336$ amostras de tamanho 3 sem reposição.

5.15 Encontre n se $P(n, 2) = 72$.

$$P(n, 2) = n(n - 1) = n^2 - n. \text{ Logo, temos}$$
$$n^2 - n = 72 \quad \text{ou} \quad n^2 - n - 72 = 0 \text{ ou } (n - 9)(n + 8) = 0$$

Como n deve ser positivo, a única resposta é $n = 9$.

Combinações

5.16 Uma classe tem 10 estudantes com 6 homens e 4 mulheres. Encontre o número n de maneiras para:

(*a*) Selecionar um comitê de 4 membros entre os estudantes.

(*b*) Selecionar um comitê de 4 membros com 2 homens e 2 mulheres.

(*c*) Eleger um presidente, um vice-presidente e um tesoureiro.

(*a*) Isso se refere a combinações e não a permutações, pois a ordem não é relevante em uma comissão. Há "10 escolhem 4" de tais comitês. Ou seja,

$$n = C(10, 4) = \binom{10}{4} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2 \cdot 1} = 210$$

(*b*) Os dois homens podem ser escolhidos a partir dos seis homens de $C(6, 2)$ maneiras, e as duas mulheres podem ser escolhidas a partir das quatro mulheres de $C(4, 2)$ maneiras. Assim, pela Regra do Produto.

$$n = \binom{6}{2}\binom{4}{2} = \frac{6\cdot 5}{2\cdot 1}\cdot\frac{4\cdot 3}{2\cdot 1} = 15(6) = 90$$

(*c*) Isso se refere a permutações e não a combinações, pois a ordem é relevante. Logo,

$$n = P(6, 3) = 6 \cdot 5 \cdot 4 = 120$$

5.17 Uma caixa contém 8 meias azuis e 6 meias vermelhas. Encontre o número de maneiras que duas meias podem ser retiradas da caixa se:

(*a*) Elas podem ser de qualquer cor. (*b*) Elas devem ser da mesma cor.

(*a*) Há "14 escolhem 2" de tais maneiras para selecionar duas das quatorze meias. Assim:

$$n = C(14, 2) = \binom{14}{2} = \frac{14\cdot 13}{2\cdot 1} = 91$$

(*b*) Há $C(8, 2) = 28$ maneiras para escolher duas das oito meias azuis, e $C(6, 2) = 15$ maneiras para escolher duas das quatro meias vermelhas. Pela Regra da Soma, $n = 28 + 15 = 43$.

5.18 Encontre o número m de comitês de 5 com um dado presidente que podem ser selecionados a partir de 12 pessoas.

O presidente pode ser escolhido de 12 maneiras e, a seguir, os outros quatro do comitê podem ser escolhidos a partir dos 11 restantes de $C(11, 4)$ maneiras. Logo, $m = 12 \cdot C(11, 4) = 12 \cdot 330 = 3960$.

Princípio da casa dos pombos

5.19 Encontre o número mínimo n de inteiros a serem selecionados de $S = \{1, 2, \ldots, 9\}$, de forma que: (*a*) A soma de dois dos n inteiros seja par. (*b*) A diferença de dois dos n inteiros seja 5.

(*a*) A soma de dois inteiros pares ou de dois inteiros ímpares é par. Considere os subconjuntos $\{1, 3, 5, 7, 9\}$ e $\{2, 4, 6, 8\}$ de S como casas de pombos. Logo, $n = 3$.

(*b*) Considere os cinco subconjuntos $\{1, 6\}$, $\{2, 7\}$, $\{3, 8\}$, $\{4, 9\}$ e $\{5\}$ de S como casas de pombos. Então, $n = 6$ garante que dois inteiros pertencem a um dos subconjuntos e suas diferenças sejam 5.

5.20 Encontre o número mínimo de estudantes universitários necessários para garantir que cinco deles pertençam à mesma turma (primeiro ano, segundo ano, terceiro ano e quarto ano).

Aqui as $n = 4$ turmas são os casas de pombos e $k + 1 = 5$, logo, $k = 4$. Assim, entre $kn + 1 = 17$ estudantes (pombos), cinco deles pertencem à mesma turma.

5.21 Seja L uma lista (não necessariamente em ordem alfabética) das 26 letras do alfabeto inglês (que consiste em 5 vogais, A, E, I, O, U, e 21 consoantes).

(*a*) Mostre que L tem uma sublista consistindo em quatro ou mais consoantes consecutivas.

(*b*) Assumindo que L começa com uma vogal, digamos A, mostre que L tem uma sublista consistindo em cinco ou mais consoantes consecutivas.

(*a*) As cinco letras particionam L em $n = 6$ sublistas (casas de pombos) de consoantes consecutivas. Aqui $k + 1 = 4$ e, assim, $k = 3$. Logo, $nk + 1 = 6(3) + 1 = 19 < 21$. Portanto, alguma sublista tem pelo menos quatro consoantes consecutivas.

(*b*) Como L começa com uma vogal, as outras vogais particionam L em $n = 5$ sublistas. Aqui $k + 1 = 5$ e, assim, $k = 4$. Logo, $kn + 1 = 21$. Portanto, alguma sublista tem pelo menos cinco consoantes consecutivas.

Princípio de inclusão-exclusão

5.22 Há 22 estudantes mulheres e 18 estudantes homens em uma sala de aula. Encontre o número total t de estudantes.

Os conjuntos de estudantes homens e mulheres são disjuntos; logo, $t = 22 + 18 = 40$.

5.23 Suponha que entre 32 pessoas que armazenam papel ou garrafas (ou ambos) para reciclagem, há 30 que armazenam papel e 14 que armazenam garrafas. Encontre o número m de pessoas que.

(*a*) armazenam ambos, (*b*) armazenam apenas papel, (*c*) armazenam apenas garrafas.

Sejam P e B os conjuntos de pessoas que armazenam papel e garrafas, respectivamente. Então:

$$(a)\ m = n(P \cap B) = n(P) + n(B) - n(P \cup B) = 30 + 14 - 32 = 12$$

$$(b)\ m = n(P \setminus B) = n(P) - n(P \cap B) = 30 - 12 = 18$$

$$(c)\ m = n(B \setminus P) = n(P) - n(P \cap B) = 14 - 12 = 2$$

5.24 Sejam A, B, C e D, respectivamente, disciplinas de arte, biologia, química e dramaturgia. Encontre o número N de estudantes em uma república, sabendo que:

12 fazem A,	5 fazem A e B,	4 fazem B e D,	2 fazem B, C e D,
20 fazem B,	7 fazem A e C,	3 fazem C e D,	3 fazem A, C e D,
20 fazem C,	4 fazem A e D,	3 fazem A, B e C,	2 fazem as quatro,
8 fazem D,	16 fazem B e C,	2 fazem A, B e D,	71 não fazem nenhuma.

Seja T o número de estudantes que fazem pelo menos uma disciplina. Pelo Princípio de Inclusão-Exclusão do Teorema 5.9, $T = s_1 - s_2 + s_3 - s_4$, onde

$$s_1 = 12 + 20 + 20 + 8 = 60, \qquad s_2 = 5 + 7 + 4 + 16 + 4 + 3 = 39,$$

$$s_3 = 3 + 2 + 2 + 3 = 10, \qquad s_4 = 2.$$

Assim, $T = 29$ e $N = 71 + T = 100$

Diagramas em árvore

5.25 Os times A e B jogam em um torneio. O primeiro time a ganhar três jogos vence a competição. Encontre o número de possíveis maneiras como o torneio pode transcorrer.

Construa o diagrama em árvore apropriado na Fig. 5-3(*a*). O torneio pode acontecer de 20 maneiras.

AAA, AABA, AABBA, AABBB, ABAA, ABABA, ABABB, ABBAA, ABBAB, ABBB,
BBB, BBAB, BBAAB, BBAAA, BABB, BABAB, BABAA, BAABB, BAABA, BAAA

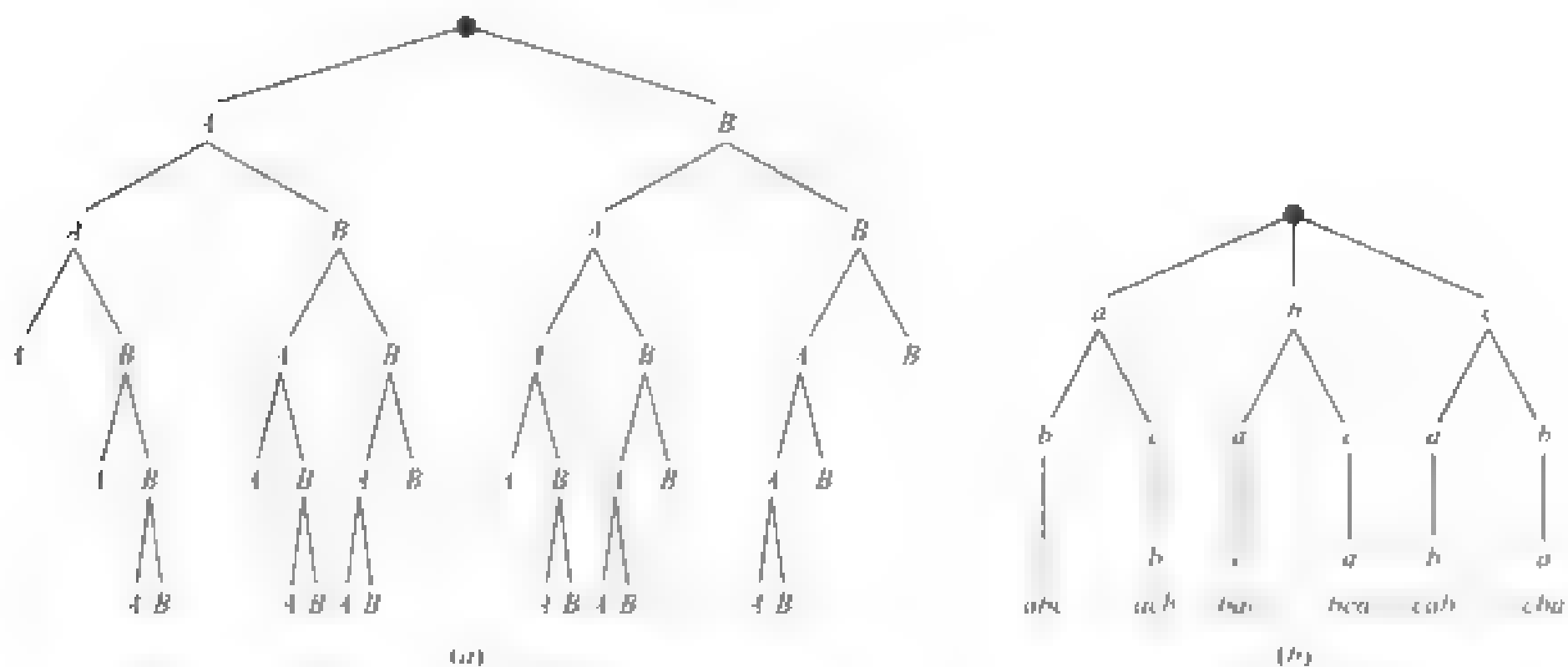



Figura 5-3

5.26 Construa o diagrama em árvore que exibe as permutações de $\{a, b, c\}$.

O diagrama em árvore aparece na Fig. 5-3(*b*). Há seis permutações e elas são listadas na parte inferior do diagrama.

Problemas variados

5.27 Existem 12 estudantes em uma turma. Encontre o número n de maneiras que os 12 estudantes podem realizar 3 testes, se 4 deles fizerem cada teste.

Há $C(12, 4) = 495$ maneiras de escolher 4 dos 12 estudantes que devem fazer o primeiro teste. Seguindo isso, existem $C(8, 4) = 70$ maneiras de escolher 4, entre os 8 estudantes restantes, para fazer o segundo teste. Os demais realizam o terceiro teste. Logo:

$$n = 70(495) = 34\,650$$

5.28 Prove o Teorema 5.2 (Teorema Binomial): $(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r$

O teorema é verdadeiro para $n = 1$, uma vez que

$$\sum_{r=0}^{1} \binom{1}{r} a^{1-r} b^r = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b = (a+b)^1$$

Assumimos que ele é verdadeiro para $(a+b)^n$ e o provamos para $(a+b)^{n+1}$.

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b)[a^n + \tbinom{n}{1} a^{n-1} b + \cdots + \tbinom{n}{r-1} a^{n-r+1} b^{r-1} + \tbinom{n}{r} a^{n-r} b^r + \cdots + \tbinom{n}{1} a b^{n-1} + b^n]\end{aligned}$$

Agora o termo no produto que contém b^r é obtido a partir de

$$\begin{aligned} b[\tbinom{n}{r-1} a^{n-r+1} b^{r-1}] + a[\tbinom{n}{r} a^{n-r} b^r] &= \tbinom{n}{r-1} a^{n-r+1} b^r + \tbinom{n}{r} a^{n-r+1} b^r \\ &= [\tbinom{n}{r-1} + \tbinom{n}{r}] a^{n-r+1} b^r \end{aligned}$$

Mas, pelo Teorema 5.3, $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$. Logo, o termo contendo b^r é:

$$\binom{n+1}{r} a^{n-r+1} b^r$$

Observe que $(a+b)(a+b)^n$ é um polinômio de grau $n+1$ em b. Consequentemente:

$$(a+b)^{n+1} = (a+b)(a+b)^n = \sum_{r=0}^{n+1} \binom{n+1}{r} a^{n-r+1} b^r$$

o que queríamos provar.

5.29 Sejam n e $n_1, n_2, \ldots, n_r$ inteiros não negativos tais que $n_1 + n_2 + \cdots + n_r = n$. Os *coeficientes multinomiais* são denotados e definidos por:

$$\binom{n}{n_1, n_2, \ldots, n_r} = \frac{n!}{n_1! n_2! \cdots n_r!}$$

Calcule os seguintes coeficientes multinomiais.

(a) $\binom{6}{3, 2, 1}$, (b) $\binom{8}{4, 2, 2, 0}$, (c) $\binom{10}{5, 3, 2, 2}$

(a) $\binom{6}{3, 2, 1} = \frac{6!}{3!2!1!} = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 1} = 60$

(b) $\binom{8}{4, 2, 2, 0} = \frac{8!}{4!2!2!0!} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 1} = 420$

(c) $\binom{10}{5, 3, 2, 2}$ não tem significado, pois $5 + 3 + 2 + 2 \neq 10$.

5.30 Um aluno deve estudar em cinco turmas de três áreas de estudo. Várias turmas são oferecidas em cada disciplina, mas ele não pode estudar em mais de duas turmas de uma dada área.

(*a*) Usando o Princípio da Casa dos Pombos, mostre que o aluno estudará em pelo menos duas turmas de uma área.

(*b*) Usando o Princípio de Inclusão-Exclusão, mostre que o aluno deverá estudar em pelo menos uma turma de cada área.

(*a*) As três áreas são as casas e o aluno deve estudar em cinco turmas (pombos). Logo, o aluno deve estudar em pelo menos duas turmas de uma área.

(*b*) Considere que as três áreas de estudo representam três conjuntos disjuntos, A, B e C. Como os conjuntos são disjuntos, $n(A \cup B \cup C) = 5 = n(A) + n(B) + n(C)$. Uma vez que o aluno deve estudar no máximo em duas turmas de qualquer área, a soma de turmas em quaisquer dois conjuntos, digamos A e B, deve ser menor ou igual a quatro. Logo, $5 - [n(A) + n(B)] = n(C) \geq 1$. Assim, o aluno deve estudar em pelo menos uma turma de qualquer área.

Problemas Complementares

Notação fatorial, coeficientes binomiais

5.31 Encontre: (a) $10!$, $11!$, $12!$, (b) $60!$ (Sugestão: Use a aproximação de Stirling para $n!$.)

5.32 Calcule: (a) $16!/14!$; (b) $14!/11!$; (c) $8!/10!$; (d) $10!/13!$.

5.33 Simplifique: (a) $\dfrac{(n+1)!}{n!}$; (b) $\dfrac{n!}{(n-2)!}$; (c) $\dfrac{(n-1)!}{(n+2)!}$; (d) $\dfrac{(n-r+1)!}{(n-r-1)!}$

5.34 Encontre: (a) $\binom{5}{2}$ (b) $\binom{7}{3}$ (c) $\binom{14}{2}$ (d) $\binom{6}{4}$ (e) $\binom{20}{17}$ (f) $\binom{18}{15}$

5.35 Mostre que: (a) $\binom{n}{0} + \binom{n}{n} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n$

(b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots \pm \binom{n}{n} = 0$

5.36 Dada a oitava linha do triângulo de Pascal a seguir, encontre: (a) a nona linha; (b) a décima linha.

$$1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1$$

5.37 Calcule os seguintes coeficientes multinomiais (definidos no Problema 5.29).

(a) $\binom{6}{2,\ 3,\ 1}$, (b) $\binom{7}{3,\ 2,\ 2,\ 0}$, (c) $\binom{9}{3,\ 5,\ 1}$, (d) $\binom{8}{4,\ 3,\ 2}$

Princípios de contagem

5.38 Uma loja vende roupas masculinas. Ela tem três tipos de jaquetas, sete tipos de camisas e cinco tipos de calças. Encontre o número de maneiras que uma pessoa pode comprar: (a) um dos itens; (b) uma peça de cada um dos três tipos de roupas.

5.39 Uma turma tem 10 alunos e 8 alunas. Encontre o número de maneiras que a turma pode eleger: (a) um(a) representante; (b) dois representantes, sendo um homem e uma mulher; (c) um(a) presidente e um(a) vice-presidente.

5.40 Suponha que um código consiste em cinco caracteres, duas letras seguidas de três dígitos. Encontre o número de: (a) códigos; (b) códigos com letras distintas; (c) códigos com as mesmas letras.

Permutações

5.41 Encontre o número de placas de carro tais que: (a) Cada placa contém duas letras diferentes seguidas por três dígitos distintos; (b) O primeiro dígito não pode ser 0.

5.42 Encontre o número m de maneiras que um árbitro pode conceder primeiro, segundo e terceiro lugar em uma competição com 18 concorrentes.

5.43 Encontre o número de maneiras que 5 livros grandes, 4 médios e 3 pequenos podem ser colocados em uma estante, de modo que: (a) não existam restrições; (b) todos os livros de mesmo tamanho estejam juntos.

5.44 Uma equipe de debate consiste em 3 meninos e 3 meninas. Encontre o número de maneiras que eles podem sentar em um banco, onde: (a) não há restrições; (b) meninos e meninas sentam um ao lado do outro; (c) apenas as meninas sentam juntas.

5.45 Encontre o número de maneiras que 5 pessoas podem sentar em um banco, onde: (a) não há restrições; (b) duas das pessoas insistem em sentar uma ao lado da outra.

5.46 Repita o Problema 5.45 se as pessoas sentam ao redor de uma mesa redonda.

5.47 Considere todos os inteiros positivos com três dígitos diferentes. (Note que zero não pode ser o primeiro dígito.) Encontre a quantia deles que são: (a) maiores do que 700; (b) ímpares; (c) divisíveis por 5.

5.48 Suponha que repetições não sejam permitidas. (a) Encontre a quantia de números de três dígitos que podem ser formados a partir de 2, 3, 5, 6, 7 e 9. (b) Quantos deles são menores do que 400? (c) Quantos deles são pares?

5.49 Encontre o número m de maneiras como 6 pessoas podem dirigir uma caminhonete se uma entre três deve conduzir.

5.50 Encontre n se: (a) $P(n, 4) = 42P(n, 2)$; (b) $2P(n, 2) + 50 = P(2n, 2)$.

Permutações com repetições, amostras ordenadas

5.51 Encontre o número de permutações que podem ser formadas a partir de todas as letras de cada palavra: (a) QUEUE; (b) COMMITTEE; (c) PROPOSITION; (c) BASEBALL.

5.52 Suponha que sejam dadas quatro bandeiras vermelhas idênticas, duas azuis idênticas e três verdes idênticas. Encontre o número m de sinais diferentes que podem ser formados, hasteando as nove bandeiras em um mastro.

5.53 Uma caixa contém 12 lâmpadas. Encontre o número n de amostras ordenadas de tamanho 3: (a) com reposição; (b) sem reposição.

5.54 Uma turma contém 10 estudantes. Encontre o número n de amostras ordenadas de tamanho 4: (a) com reposição; (b) sem reposição.

Combinações

5.55 Um restaurante tem 6 tipos diferentes de sobremesa. Encontre o número de maneiras que um cliente pode escolher: (a) uma sobremesa; (b) duas sobremesas; (c) três sobremesas.

5.56 Uma turma contém 9 homens e 3 mulheres. Encontre o número de maneiras que um professor pode selecionar um comitê de 4, a partir da turma, onde há:

(a) nenhuma restrição; (b) dois homens e duas mulheres; (c) exatamente uma mulher; (d) pelo menos uma mulher.

5.57 Uma mulher tem 11 amigos próximos. Encontre o número de maneiras que ela pode convidar 5 deles para jantar, onde:

(a) Não há restrições.

(b) Dois dos amigos são casados entre si e não jantarão separadamente.

(c) Dois dos amigos não estão falando um com o outro e não jantarão juntos.

5.58 Uma turma contém 8 homens e 6 mulheres, na qual há um casal casado. Encontre o número m de maneiras que um professor pode selecionar um comitê de 4, a partir da turma, onde o marido ou a esposa, mas não ambos, podem participar do comitê.

5.59 Uma caixa tem 6 meias azuis e 4 brancas. Encontre o número de maneiras que duas meias podem ser retiradas da caixa, onde:

(a) Não há restrições. (b) Elas têm cores diferentes. (c) Elas têm a mesma cor.

5.60 Uma aluna deve responder a 10 entre 13 questões. Encontre o número de suas escolhas, de modo que ela deve responder:

(a) às duas primeiras questões; (c) exatamente a 3 entre às 5 primeiras questões;

(b) à primeira questão ou à segunda, mas não a ambas, (d) pelo menos à 3 das 5 primeiras questões.

Princípio de Inclusão-Exclusão

5.61 Suponha que 32 estudantes estão em uma turma A de artes e 24 estão em uma turma B de biologia, e suponha que 10 estão em ambas as turmas. Encontre o número de estudantes que estão:

(a) na turma A ou na B; (b) apenas na turma A, (c) apenas na turma B

5.62 Uma pesquisa entre 80 proprietários de carros mostra que 24 possuem um veículo importado e 60 possuem um nacional. Encontre o número de proprietários que têm:

(a) tanto um carro importado quanto um nacional.

(b) apenas um carro importado.

(c) apenas um carro nacional.

5.63 Considere todos os inteiros de 1 a 100, inclusive. Encontre a quantia deles que são.

(a) ímpares ou quadrados de inteiros; (b) pares ou cubos de inteiros.

5.64 Em uma turma de 30 estudantes, 10 conseguiram nota máxima no primeiro teste, 9 conseguiram nota máxima no segundo teste e 15 não obtiveram esta nota em nenhuma das avaliações. Encontre: o número de estudantes que conseguiram

(a) nota máxima em ambos os testes.

(b) nota máxima no primeiro teste, mas não no segundo.

(c) nota máxima no segundo teste, mas não no primeiro.

5.65 Considere todos os inteiros de 1 a 300, inclusive. Encontre a quantia deles que é divisível por:

(a) pelo menos 3, 5 ou 7; (c) 5, mas não por 3 ou 7.

(b) 3 e 5, mas não por 7; (d) por nenhum dos números 3, 5 e 7.

5.66 Em uma certa escola, francês (F), espanhol (E) e alemão (A) são as únicas línguas estrangeiras lecionadas. Entre 80 estudantes,

(i) 20 estudam F, 25 estudam E, 15 estudam A

(ii) 8 estudam F e E, 6 estudam E e A, 5 estudam F e A.

(iii) 2 estudam as três línguas.

Encontre a quantia, entre os 80 estudantes, que estuda:

(a) nenhuma das línguas, (c) apenas uma língua, (e) exatamente duas dessas línguas.

(b) apenas francês; (d) apenas espanhol e alemão;

5.67 Encontre o número m de elementos na união dos conjuntos A, B, C e D com as quatro condições a seguir:

(i) A, B, C e D têm 50, 60, 70 e 80 elementos, respectivamente.

(ii) Cada par de conjuntos tem 20 elementos em comum.

(iii) Cada tripla de conjuntos tem 10 elementos em comum.

(iv) Os quatro conjuntos têm 5 elementos em comum.

Princípio da Casa dos Pombos

5.68 Encontre o número mínimo de estudantes necessários para garantir que quatro deles nasceram. (a) no mesmo dia da semana; (b) no mesmo mês.

5.69 Encontre o número mínimo de estudantes necessários para garantir que três deles:

(a) têm sobrenomes que começam com a mesma letra;

(b) nasceram no mesmo dia de um mês (com 31 dias).

5.70 Considere um torneio com n jogadores, no qual cada um joga contra os demais. Suponha que cada jogador vença pelo menos uma vez. Mostre que pelo menos dois dos jogadores têm o mesmo número de vitórias.

5.71 Suponha que 5 pontos sejam escolhidos ao acaso no interior de um triângulo equilátero T, onde cada lado tem comprimento de duas polegadas. Mostre que a distância entre dois dos pontos deve ser menor do que uma polegada.

5.72 Considere um conjunto qualquer $X = \{x_1, x_2, \ldots, x_7\}$ de sete inteiros distintos. Mostre que existem $x, y \in X$ tais que $x + y$ ou $x - y$ é divisível por 10.

Problemas variados

5.73 Encontre o número m de maneiras que dez estudantes podem ser divididos em três times, em que um deles tem quatro pessoas e os outros têm três.

5.74 Assumindo que uma célula pode ser vazia, encontre o número n de maneiras que um conjunto com três elementos pode ser particionado em: (a) 3 células ordenadas, (b) 3 células não ordenadas.

5.75 Assumindo que uma célula pode ser vazia, encontre o número n de maneiras que um conjunto com quatro elementos pode ser particionado em: (a) 3 células ordenadas; (b) 3 células não ordenadas.

5.76 O alfabeto inglês tem 26 letras, das quais cinco são vogais. Considere apenas "palavras" de cinco letras consistindo em três consoantes diferentes e duas vogais distintas. Encontre a quantia dessas palavras, tais que:

(a) não há restrições; (c) elas contêm as letras B e C;

(b) elas contêm a letra B; (d) elas começam com B e contêm a letra C.

5.77 Os times A e B jogam no campeonato mundial de beisebol, no qual o primeiro time que ganhar quatro jogos vence o campeonato. Suponha que A vence o primeiro jogo e que o time que ganha o segundo jogo tem vitória também no quarto jogo.

(a) Encontre e liste o número n de maneiras que o campeonato pode ocorrer.

(b) Encontre o número de maneiras que B vence o campeonato.

(c) Encontre o número de maneiras que o campeonato pode durar sete jogos.

5.78 Encontre o número de maneiras que uma moeda pode ser jogada:

(a) seis vezes, de modo que há exatamente três caras e duas caras jamais ocorrem consecutivamente.

(b) $2n$ vezes, de modo que há exatamente n caras e duas caras jamais ocorrem consecutivamente.

5.79 Encontre o número de maneiras que três elementos a, b e c podem ser associados a três células, de modo que exatamente uma célula fica vazia.

5.80 Encontre o número de maneiras que n elementos distintos podem ser associados a n células, de modo que exatamente uma célula fica vazia.

Respostas dos Problemas Complementares

5.31 (a) 3 628 800; 39 916 800; 479 001 600;

(b) $\log(60!) = 81{,}92$, logo $60! = 6{,}59 \times 10^{81}$.

5.32 (a) 240; (b) 2 184, (c) 1/90; (d) 1/1716.

5.33 (a) $n + 1$; (b) $n(n - 1)$; (c) $1/[n(n + 1)(n + 2)]$; (d) $(n - r)(n - r + 1)$.

5.34 (a) 10; (b) 35, (c) 91, (d) 15, (e) 1140; (f) 816.

5.35 Sugestões: (a) Expandir $(1 + 1)^n$; (b) Expandir $(1 - 1)^n$.

5.36 (a) 1, 9, 36, 84, 126, 126, 84, 36, 9, 1; (b) 1, 10, 45, 120, 210, 252, 210, 120, 45, 10, 1.

5.37 (a) 60; (b) 210; (c) 504, (d) não definido.

5.38 (a) 15; (b) 105.

5.39 (a) 18; (b) 80; (c) 306.

5.40 (a) $26^2 \cdot 10^3$; (b) $26 \cdot 25 \cdot 10^3$; (c) $26 \cdot 10^3$.

5.41 (a) $26 \cdot 25 \cdot 10 \cdot 9 \quad 8 = 468\,000$; (b) $26 \quad 25 \cdot 9 \quad 9 \cdot 8 = 421\,200$.

5.42 $m = 18 \cdot 17 \cdot 16 = 4896$.

5.43 (a) 12!; (b) 3!5!4!3! = 103 680.

5.44 (a) 6! = 720; (b) $2 \cdot 3! \cdot 3! = 72$; (c) $4 \cdot 3! \cdot 3! = 144$.

5.45 (a) 120; (b) 48.

5.46 (a) 24, (b) 12.

5.47 (a) 3 9 8, (b) 9 8 5; (c) 9 8 7/2, (d) 9 8 7/5

5.48 (a) $P(6, 3) = 120$; (b) $2 \quad 5 \cdot 4 = 40$; (c) $2 \cdot 5 \cdot 4 = 40$.

5.49 $m = 360$

5.50 (a) 9; (b) 5.

5.51 (a) 30; (b) 9!/[2!2!2!] = 45 360; (c) 11!/[2!3!2!] = 1 663 200, (d) 8!/[2!2!2!] = 5040.

5.52 m = 9!/[4 2!3!] = 1260.

5.53 (a) $12^3 = 1\,728$, (b) $P(12, 3) = 1320$.

5.54 (a) $10^4 = 10\,000$; (b) $P(10, 4) = 5040$.

5.55 (a) 6; (b) 15; (c) 20.

5.56 (a) $C(12, 4)$; (b) $C(9, 2) \quad C(3, 2) = 108$, (c) $C(9, 3) \quad 3 = 252$, (d) $9 + 108 + 252 = 369$ ou $C(12, 4) \quad C(9, 4) = 369$

5.57 (a) $C(11, 5) = 462$; (b) $126 + 84 = 210$; (c) $C(9, 5) + 2C(9, 4) = 378$.

5.58 $m = C(12, 4) + 2C(12, 3) = 935$.

5.59 (a) $C(10, 2) = 45$; (b) $6 \cdot 4 = 24$, (c) $C(6, 2) + C(4, 2) = 21$ ou $45 - 24 = 21$.

5.60 (a) 165; (b) 110; (c) 80; (d) 276

5.61 (a) 46; (b) 22; (c) 14

5.62 (a) 4, (b) 20; (c) 56.

5.63 (a) 55; (b) 52.

5.64 (a) 4, (b) 6; (c) 5

5.65 (a) $100 + 60 + 42 - 20 - 14 - 8 + 2 = 162$, (b) $20 - 2 = 18$, (c) $60 - 20 - 8 + 2 = 34$, (d) $300 - 162 = 138$.

5.66 (a) 37; (b) 9; (c) 28; (d) 4; (e) 13

5.67 $m = 175$.

5.68 (a) 22; (b) 37.

5.69 (a) 53; (b) 63.

5.70 Cada jogador vencerá de 1 a $n - 1$ jogos (casas). Há n jogadores (pombos).

5.71 Esboce três segmentos de reta entre os pontos médios dos lados de T. Isso particiona T em quatro triângulos equiláteros (casas), onde cada lado tem comprimento 1. Dois dos cinco pontos (pombos) devem estar sobre um dos triângulos.

5.72 Seja r_i o resto quando x_i é divisível por 10. Considere as seis casas de pombos $H_1 = \{x_i \mid r_i = 0\}$, $H_2 = \{x_i \mid r_i = 5\}$, $H_3 = \{x_i \mid r_i = 1 \text{ ou } 9\}$, $H_4 = \{x_i \mid r_i = 2 \text{ ou } 8\}$, $H_5 = \{x_i \mid r_i = 3 \text{ ou } 7\}$, $H_6 = \{x_i \mid r_i = 4 \text{ ou } 6\}$. Então, algum x e y pertence a algum H_k.

5.73 $m = C(10, 4) \cdot C(6, 3) = 420$

5.74 (a) $n = 3^3 = 27$ (Cada elemento pode ser colocado em qualquer uma das três células.) (b) O número de elementos em três células pode ser distribuído como se segue: [3, 0, 0], [2,1,0], ou [1,1,1]. Logo, $n = 1 + 3 + 1 = 5$

5.75 (a) $n = 3^4 = 81$ (Cada elemento pode ser colocado em qualquer uma das três células.) (b) O número de elementos em três células pode ser distribuído como se segue. [4, 0, 0], [3, 1, 0], [2, 2, 0], ou [2, 1, 1]. Logo, $n = 1 + 4 + 3 + 6 = 14$.

5.76 (a) $C(21, 3) \cdot C(5, 2) \cdot 5!$, (b) $C(20, 2) \cdot C(5, 2) \cdot 5!$; (c) $19 \cdot C(5, 2) \cdot 5!$, (d) $19 \cdot C(5, 2) \cdot 4!$.

5.77 Esboce o diagrama em árvore T como na Fig. 5-4. Observe que T começa em A, o vencedor do primeiro jogo, e há apenas uma escolha no quarto jogo, o vencedor da segunda partida.

(a) $n = 15$, como listado abaixo; (b) 6; (c) 8. *AAAA*, *AABAA*, *AABABA*, *AABABBA*, *AABABBB*, *ABABAA*, *ABABABA*, *ABABABB*, *ABABBAA*, *ABABBAB*, *ABABBB*, *ABBBAAA*, *ABBBAAB*, *ABBBAB*, *ABBBB*

5.78 (a) 4, *HTHTHT*, *HTTHTH*, *HTHTTH*, *THTHTH*; (b) $n + 1$.

5.79 18

5.80 $n!C(n, 2)$.

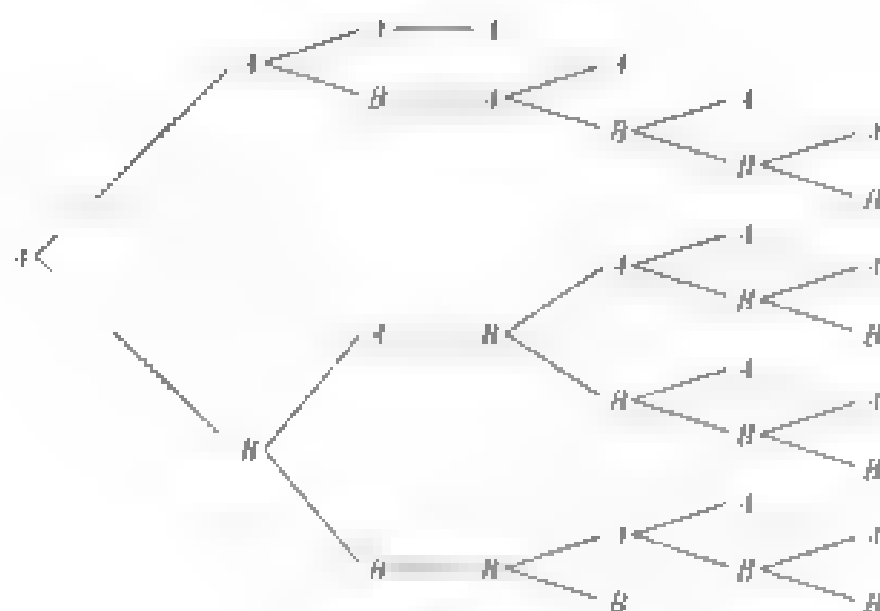



Figura 5-4

Técnicas Avançadas de Contagem, Recursão

6.1 INTRODUÇÃO

Consideramos aqui técnicas de contagem e problemas mais sofisticados. Isso inclui problemas envolvendo combinações com repetições, partições ordenadas e não ordenadas, e os princípios de Inclusão-Exclusão e da Casa dos Pombos.

Também discutimos recursão neste capítulo.

6.2 COMBINAÇÕES COM REPETIÇÕES

Considere o seguinte problema. Uma confeitaria faz apenas $M = 4$ tipos de biscoitos: maçã (a), banana (b), cenoura (c) e tâmaras (d). Encontre o número de maneiras que uma pessoa pode comprar $r = 8$ biscoitos.

Observe que a ordem não é relevante. Esse é um exemplo de combinações com repetições. Em particular, cada combinação pode ser listada com os a's primeiro, seguidos dos b's, dos c's e, finalmente, dos d's. Quatro dessas combinações seguem.

$$r_1 = aa, bb, cc, dd; \; r_2 = aaa, c, ddd; \; r_3 = bbbb, c, ddd; \; r_4 = aaaaa, ddd.$$

Contar o número m de tais combinações pode não ser fácil.

Suponha que desejamos codificar as combinações acima usando apenas dois símbolos, digamos 0 e 1. Isso pode ser feito com 0 denotando um biscoito e 1 denotando uma mudança de um tipo de biscoito para outro. Então cada combinação requer $r = 8$ zeros, um para cada biscoito, e $M - 1 = 3$ uns, onde o primeiro denota a mudança de a para b, o segundo de b para c, e o terceiro de c para d. Assim, as quatro combinações são codificadas como se segue.

$$r_1 = 00100100100, \; r_2 = 00001101000, \; r_3 = 10000101000, \; r_4 = 00000111000.$$

Contar o número m dessas "palavras codificadas" é fácil. Cada palavra codificada contém $R + M - 1 = 11$ dígitos, onde $r = 8$ são 0's e, portanto, $M - 1 = 3$ são 1's. Consequentemente,

$$M = C(11, 8) = C(11, 3) = \frac{11 \cdot 10 \cdot 9}{3 \cdot 2 \cdot 1} = 165$$

Um argumento semelhante nos dá o teorema a seguir.

Teorema 6.1: Suponha que há M tipos de objetos. Então o número de combinações de r desses objetos é $C(r + M - 1, r) = C(r + M - 1, M - 1)$.

Exemplo 6.1 Encontre o número m de soluções inteiras não negativas de $x + y + z = 18$.

Podemos ver cada solução, digamos, $x = 3$, $y = 7$, $z = 8$, como uma combinação de $r = 18$ objetos consistindo em 3 a's, 7 b's e 8 c's, onde existem $M = 3$ tipos de objetos, a's, b's e c's. Pelo Teorema 6.1,

$$m = C(r + M - 1, M - 1) = C(20, 2) = 190.$$

6.3 PARTIÇÕES ORDENADAS E NÃO ORDENADAS

Suponha que um conjunto S tem 7 elementos. Queremos encontrar o número m de partições ordenadas de S em três células, digamos, $[A_1, A_2, A_3]$, de forma que elas contenham 2, 3 e 2 elementos, respectivamente.

Como S tem 7 elementos, há $C(7, 2)$ maneiras de escolher os dois primeiros elementos para A_1. Seguindo isso, há $C(5, 3)$ maneiras de escolher os três elementos para A_2. Por último, existem $C(2, 2)$ maneiras de escolher os dois elementos para A_3 (ou, os dois últimos elementos da célula A_3). Assim:

$$m = C(7, 2)C(5, 3)C(2, 2) = \binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7 \cdot 6}{2 \cdot 1} \cdot \frac{5 \cdot 4 \cdot 3}{3 \cdot 2 \cdot 1} \cdot \frac{2 \cdot 1}{2 \cdot 1} = 210$$

Observe que

$$m = \binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7!}{2!5!} \cdot \frac{5!}{3!2!} \cdot \frac{2!}{2!0!} = \frac{7!}{2!3!2!}$$

uma vez que cada numerador após o primeiro é cancelado por um termo no denominador do fator anterior.

Tal discussão pode ser mostrada como sendo verdadeira no caso geral. Ou seja:

Teorema 6.2: O número m de partições ordenadas de um conjunto S com n elementos em r células $[A_1, A_2, \ldots, A_r]$, onde, para cada i, $n(A_i) = n_i$, segue abaixo:

$$m = \frac{n!}{n_1! n_2! \cdots n_r!}$$

Partições não ordenadas

Frequentemente, queremos particionar um conjunto S em células $[A_1, A_2, \ldots, A_r]$, onde as células são agora não ordenadas. O número m' de tais partições não ordenadas é obtido a partir do número m' de partições ordenadas, dividindo m' por $k!$, onde k das células têm o mesmo número de elementos.

Exemplo 6.2 Encontre o número m de maneiras para particionar 10 estudantes em quatro times $[A_1, A_2, A_3, A_4]$, de forma que dois times têm 3 estudantes e dois têm 2 estudantes.

Pelo Teorema 6.2, há $m' = 10!/(3!3!2!2!) = 25\,200$ dessas partições ordenadas.

Como os times formam uma partição não ordenada, dividimos m' por 2! por causa das duas células com 3 elementos cada e 2! por causa das duas células com 2 elementos cada.

Assim, $m = 25\,200/(2!2!) = 6300$.

6.4 PRINCÍPIO DE INCLUSÃO-EXCLUSÃO REVISITADO

Sejam $A_1, A_2, \ldots, A_r$ subconjuntos de um conjunto universo U. Suponha que s_k denota a soma das cardinalidades de todas as possíveis k-uplas interseções dos conjuntos, ou seja, a soma de todas as cardinalidades

$$n(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k})$$

Por exemplo,

$$s_1 = \sum_i n(A_i), \quad s_2 = \sum_{i<j} n(A_i \cap A_j), \quad s_3 = \sum_{i_1 < i_2 < i_3} n(A_{i_1} \cap A_{i_2} \cap A_{i_3})$$

O Princípio de Inclusão-Exclusão, que aparece na Seção 5.7, fornece uma fórmula para o número de elementos na união dos conjuntos. Especificamente, (Teorema 5.9) temos

$$n(A_1 \cup A_2 \cup \cdots \cup A_r) = s_1 - s_2 + s_3 - \cdots + (-1)^{r-1} s_r$$

Por outro lado, usando a Lei de DeMorgan,

$$n(A_1^C \cap A_2^C \cap \ldots \cap A_r^C) = n([A_1 \cup A_2 \cup \cdots \cup A_r]^C) = |\mathrm{U}| - n(A_1 \cup A_2 \cup \cdots \cup A_r)$$

Logo, obtemos uma forma alternativa para o Teorema 5.9:

Teorema (Princípio de Inclusão-Exclusão) 6.3: Sejam $A_1, A_2, \ldots, A_r$ subconjuntos de um conjunto universo U. Então o número m de elementos que não aparecem em qualquer um dos subconjuntos $A_1, A_2, \ldots, A_r$ de U é.

$$m = n(A_1^C \cap A_2^C \cap \cdots \cap A_r^C) = |\mathrm{U}| - s_1 + s_2 - s_3 + \cdots + (-1)^r s_r$$

Exemplo 6.3: Seja U o conjunto de inteiros positivos que não excedem 1000. Então, $|U| = 1000$. Encontre $|S|$, onde S é o conjunto de tais inteiros que não são divisíveis por 3, 5 ou 7.

Seja A o subconjunto dos inteiros que são divisíveis por 3, B o dos divisíveis por 5, e C o dos divisíveis por 7. Então, $S = A^C \cap B^C \cap C^C$, uma vez que cada elemento de S não é divisível por 3, 5 ou 7. Por divisão inteira,

$$|A| = 1000/3 = 333, \ |B| = 1000/5 = 200, \ |C| = 1000/7 = 142,$$
$$|A \cap B| = 1000/15 = 66, \ |A \cap C| = 1000/21 = 47, \ |B \cap C| = 1000/35 = 28,$$
$$|A \cap B \cap C| = 1000/105 = 9$$

Assim, pelo Princípio da Inclusão-Exclusão, Teorema 6.3,

$$|S| = 1000 - (333 + 200 + 142) + (66 + 47 + 28) - 9 = 1000 - 675 + 141 - 9 = 457$$

Número de funções sobrejetoras

Sejam A e B conjuntos tais que $|A| = 6$ e $|B| = 4$. Queremos encontrar o número de funções sobrejetoras de A em B.

Sejam b_1, b_2, b_3 e b_4 os quatro elementos de B. Seja U o conjunto de todas as funções de A em B. Além disso, seja F_1 o conjunto de funções que não associam qualquer elemento de A a b_1, isto é, b_1 não está na imagem de qualquer função de F_1. Analogamente, sejam F_2, F_3 e F_4 os conjuntos de funções que não associam qualquer elemento de A a b_2, b_3 e b_4, respectivamente.

Estamos procurando o número de funções de $S = F_1^C \cap F_2^C \cap F_3^C \cap F_4^C$, ou seja, aquelas funções que não associam pelo menos um elemento de A a b_1, pelo menos um elemento de A a b_2, e assim por diante. Usamos o Princípio de Inclusão-Exclusão como se segue:

(i) Para cada função de U, há quatro escolhas para cada um dos 6 elementos de A, logo, $|U| = 4^6 = 4096$.

(ii) Há $C(4, 1) = 4$ funções F_i. Em cada caso, existem três escolhas para cada um dos 6 elementos em A, logo, $|F_i| = 3^6 = 729$.

(iii) Há $C(4, 2) = 6$ pares $F_i \cap F_j$. Em cada caso, existem duas escolhas para cada um dos 6 elementos de A; logo, $|F_i \cap F_j| = 2^6 = 64$.

(iv) Há $C(4, 3) = 4$ triplas $F_i \cap F_j \cap F_k$. Em cada caso existe apenas uma escolha para cada um dos 6 elementos de A. Logo, $|F_i \cap F_j \cap F_k| = 1^6 = 1$.

(v) $F_1 \cap F_2 \cap F_3 \cap F_4$ não tem elementos, ou seja, é vazio. Logo, $|F_1 \cap F_2 \cap F_3 \cap F_4| = 0$. Pelo Princípio de Inclusão-Exclusão do Teorema 6.3,

$$|S| = |F_1^C \cap F_2^C \cap F_3^C \cap F_4^C| = 4^6 - C(4, 1)3^6 + C(4, 2)2^6 - C(4, 3)1^7$$
$$= 4096 - 2916 + 384 - 1 = 795$$

O resultado acima é verdadeiro no caso geral. Assim:

Teorema 6.4: Suponha que $|A| = m$ e $|B| = n$, onde $m \geq n$. Então o número N de funções sobrejetoras de A em B é:

$$N = n^m - C(n, 1)(n-1)^m + C(n, 2)(n-2)^m - \cdots + (-1)^{n-1}C(n, n-1)1^m$$

Desarranjos

Um *desarranjo* é uma permutação de objetos na qual cada objeto não está em sua posição original. Por exemplo, 453162 não é um desarranjo de 123456, uma vez que 3 está em sua posição correta, mas 264531 é um desarranjo de 123456. (Alternativamente, uma permutação $\sigma: X \to X$ é um desarranjo se $\sigma(i) \neq i$, para todo $i \in X = \{1, 2, \ldots, n\}$.)

Seja D_n o número de desarranjos de n objetos. Por exemplo, 231 e 312 são os únicos desarranjos de 123. Logo, $D_3 = 2$. O teorema a seguir, demonstrado no Problema 6.6, se aplica.

Teorema 6.5: $D_n = n![1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}]$

A probabilidade (Capítulo 7) de que um desarranjo de n objetos ocorra é igual a D_n dividido por $n!$, o número de permutações dos n objetos. Assim, o Teorema 6.5 nos leva ao:

Corolário 6.6: Seja p a probabilidade de um desarranjo de n objetos. Então

$$p = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}$$

Exemplo 6.4 (Problema do Guarda-Chapéu) Suponha que $n = 5$ pessoas guardam seus chapéus em um restaurante e os recebem de volta ao acaso. Encontre a probabilidade p de que nenhuma pessoa receba seu próprio chapéu.

Esse é um exemplo de um desarranjo com $n = 5$. Pelo Corolário 6.6,

$$p = 1 - 1 + 1/2 - 1/6 + 1/24 - 1/120 = 44/120 = 11/30 \approx 0{,}367$$

Observe que os sinais se alternam e os termos se tornam muito pequenos no Corolário 6.6. A Fig. 6-1 fornece os valores de p para os primeiros poucos valores de n. Note que, para $n > 4$, p é muito próximo do seguinte valor (onde $e = 2{,}718$):

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} + \cdots \approx 0{,}368$$

n	1	2	3	4	5	6	7
$p = D_n/n!$	0,0000	0,5000	0,3333	0,3750	0,3667	0,3681	0,3679

Figura 6-1

6.5 PRINCÍPIO DA CASA DOS POMBOS REVISITADO

O Princípio da Casa dos Pombos (com sua generalização) é estabelecido com exemplo simples na Seção 5.6. Aqui fornecemos exemplos de aplicações mais sofisticadas desse princípio.

Exemplo 6.5 Considere seis pessoas, onde quaisquer duas delas são amigas ou desconhecidas. Mostre que há três delas que são amigas mútuas ou desconhecidas mútuas.

Seja A uma das pessoas. Sejam X consistindo naquelas que são amigas de A e Y naquelas que são desconhecidas de A. Pelo Princípio da Casa dos Pombos, X ou Y tem pelo menos três pessoas. Suponha que X tem três pessoas. Se duas delas são amigas, então as duas com A são três amigas mútuas. Caso contrário, então X tem três desconhecidas mútuas. Alternativamente, suponha que Y tem três pessoas. Se duas delas são desconhecidas, então as duas com A são três desconhecidas mútuas. Caso contrário, X tem três amigas mútuas.

Exemplo 6.6 Considere cinco pontos *reticulados* $(x_1, y_1), \ldots, (x_5, y_5)$ no plano, isto é, pontos com coordenadas inteiras. Mostre que o ponto médio de um par desses pontos é também reticulado.

O ponto médio de $P(a, b)$ e $Q(c, d)$ é $([a + c]/2, [b + d]/2)$. Observe que $(r + s)/2$ é um inteiro se r e s são inteiros com a mesma *paridade*, ou seja, ambos são ímpares ou pares. Há quatro pares de paridades: (ímpar, ímpar), (ímpar, par), (par, ímpar) e (par, par). Existem cinco pontos. Pelo Princípio da Casa dos Pombos, dois dos pontos têm o mesmo par de paridades. O ponto médio desses dois pontos tem coordenadas inteiras.

Uma aplicação importante do Princípio da Casa dos Pombos é a seguinte.

Teorema 6.7: Toda sequência de $n^2 + 1$ números reais distintos contém uma subsequência de comprimento $n + 1$, que é estritamente crescente ou estritamente decrescente.

Por exemplo, considere a seguinte sequência de $10 = 3^2 + 1$ números (onde $n = 3$): 2, 1, 8, 6, 7, 5, 9, 4, 12, 3. Há muitas subsequências de comprimento $n + 1 = 4$ que são estritamente crescentes ou estritamente decrescentes, por exemplo,

$$2, 6, 9, 12; \quad 1, 5, 9, 12; \quad 8, 6, 5, 4; \quad 7, 5, 4, 3.$$

Por outro lado, a seguinte sequência de $9 = 3^2$ números não admite subsequência de comprimento $n + 1 = 4$ que seja estritamente crescente ou estritamente decrescente:

$$3, \quad 2, \quad 1, \quad 6, \quad 5, \quad 4, \quad 9, \quad 8, \quad 7$$

A demonstração do Teorema 6.7 aparece no Problema 6.10.

6.6 RELAÇÕES DE RECORRÊNCIA

Discutimos previamente funções recursivamente definidas como

(a) Função fatorial, (b) Sequência de Fibonacci, (c) Função de Ackermann.

Discutimos aqui certos tipos de sequências $\{a_n\}$ recursivamente definidas e suas soluções. Observamos que uma *sequência* é simplesmente uma função cujo domínio é

$$\mathbf{N} = \{1, 2, 3, \ldots\} \text{ ou } \mathbf{N}_0 = \mathbf{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$$

Começamos com alguns exemplos.

Exemplo 6.7 Considere a sequência a seguir que começa com o número 3 e para a qual cada um dos termos seguintes é encontrado multiplicando o anterior por 2:

$$3, \quad 6, \quad 12, \quad 24, \quad 48, \ldots$$

Ela pode ser recursivamente definida por

$$a_0 = 3, \quad a_k = 2a_{k-1} \text{ para } k \geq 1 \quad \text{ou} \quad a_0 = 3, \quad a_{k+1} = 2a_k \quad \text{para } k \geq 0$$

A segunda definição pode ser obtida a partir da primeira, fazendo $k = k + 1$. Claramente, a fórmula $a_n = 3(2^n)$ nos fornece o n-ésimo termo da sequência sem calcular qualquer termo anterior.

As observações a seguir sobre o último exemplo são importantes.

(1) A equação $a_k = 2a_{k-1}$ ou, equivalentemente, $a_{k+1} = 2a_k$, onde um termo da sequência é definido a partir dos anteriores, é chamada de *relação de recorrência*.

(2) A equação $a_0 = 3$, que nos dá um valor específico para um dos termos, é chamada de *condição inicial*.

(3) A função $a_n = 3(2^n)$, que fornece uma fórmula para a_n como uma função de n, e não de termos anteriores, é chamada de *solução* da relação de recorrência.

(4) Pode haver muitas sequências que satisfazem uma dada relação de recorrência. Por exemplo, cada uma das seguintes é uma solução da relação de recorrência $a_k = 2a_{k-1}$.

$$1, 2, 4, 8, 16, \ldots \quad \text{e} \quad 7, 14, 28, 56, 112, \ldots$$

Todas essas soluções formam a chamada *solução geral* da relação de recorrência.

(5) Por outro lado, pode haver uma única solução para uma relação de recorrência que também satisfaça condições iniciais dadas. Por exemplo, a condição inicial $a_0 = 3$ conduz univocamente à solução 3, 6, 12, 24, . . . da relação de recorrência $a_k = 2a_{k-1}$.

Este capítulo mostra como resolver certas relações de recorrência. Primeiro, apresentamos duas sequências importantes que o leitor pode ter estudado anteriormente.

Exemplo 6.8

(a) *Progressão Aritmética*

Uma progressão aritmética é uma sequência da forma

$$a, a + d, a + 2d, a + 3d,$$

Isto é, a sequência começa com o número a e cada termo sucessivo é obtido do anterior adicionando d (a diferença comum entre dois termos quaisquer). Por exemplo:

(i) $a = 5, d = 3$: 5, 8, 9, 11, . . .

(ii) $a = 2, d = 5$: 2, 7, 12, 17, . . .

(iii) $a = 1, d = 0$: 1, 1, 1, 1, 1, . . .

Notamos que a progressão aritmética geral pode ser definida recursivamente por:

$$a_1 = a \quad \text{e} \quad a_{k+1} = a_k + d \quad \text{para} \quad k \geq 1$$

onde a solução é $a_n = a + (n - 1)d$

(b) *Progressão Geométrica*

Uma progressão geométrica é uma sequência da forma

$$a, ar, ar^2, ar^3, \ldots$$

Ou seja, a sequência inicia com o número a e cada termo sucessivo é obtido do anterior multiplicando-o por r (a razão comum entre dois termos quaisquer). Por exemplo:

(i) $a = 1, r = 3$ 1, 3, 9, 27, 81, . . .

(ii) $a = 5, r = 2$. 5, 10, 20, 40, . . .

(iii) $a = 1, r = \frac{1}{2}$. 1, $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$, . . .

Observamos que a progressão geométrica geral pode ser definida recursivamente por:

$$a_1 = a \quad \text{e} \quad a_{k+1} = ra_k + d \quad \text{para} \quad k \geq 1$$

onde a solução é $a_{n+1} = ar^n$.

6.7 RELAÇÕES DE RECORRÊNCIA LINEAR COM COEFICIENTES CONSTANTES

Uma *relação de recorrência de ordem k* é uma função da forma

$$a_n = \Phi\,(a_{n-1}, a_{n-2}, \ldots, a_{n-k}, n)$$

ou seja, onde o n-ésimo termo a_n de uma sequência é uma função dos k termos precedentes $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$ (e possivelmente n). Em particular, uma *relação de recorrência linear de k-ésima ordem com coeficientes constantes* é uma relação de recorrência da forma

$$a_n = C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} + f(n)$$

onde $C_1, C_2, \ldots, C_k$ são constantes com $C_k \neq 0$, e $f(n)$ é uma função de n. Os significados dos nomes linear e coeficientes constantes são os que se seguem:

Linear: Não há potências ou produtos dos a_j's.

Coeficientes constantes: Os $C_1, C_2, \ldots, C_k$ são constantes (não dependendem de n).

Se $f(n) = 0$, então a relação é também dita *homogênea*.

Fica claro que podemos isolar univocamente a_n se conhecemos os valores de $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$. Consequentemente, por indução matemática, há uma única sequência satisfazendo a relação de recorrência se forem dados *valores iniciais* para os primeiros k elementos da sequência.

Exemplo 6.9 Considere cada uma das seguintes relações de recorrência.

(a) $a_n = 5a_{n-1} - 4a_{n-2} + n^2$

Essa é uma relação de recorrência de segunda ordem com coeficientes constantes. É não homogênea por conta do n^2. Suponha que sejam dadas condições iniciais $a_1 = 1, a_2 = 2$. Então podemos encontrar sequencialmente os próximos elementos da sequência:

$$a_3 = 5(2) - 4(1) + 3^2 = 15, \quad a_4 = 5(15) - 4(2) + 4^2 = 83$$

(b) $a_n = 2a_{n-1}a_{n-2} + n^2$

O produto $a_{n-1}a_{n-2}$ significa que a relação de recorrência é não linear. Dadas condições iniciais $a_1 = 1, a_2 = 2$, ainda podemos determinar os próximos elementos da sequência:

$$a_3 = 2(2)(1) + 3^2 = 13, \quad a_4 = 2(13)(2) + 4^2 = 68$$

(c) $a_n = na_{n-1} + 3a_{n-2}$

Essa é uma relação de recorrência linear homogênea de segunda ordem, mas não do tipo que tem coeficientes constantes, pois o coeficiente a_{n-1} é n, que não é constante. Dadas as condições iniciais $a_1 = 1, a_2 = 2$, os próximos elementos da sequência são os seguintes:

$$a_3 = 3(2) + 3(1) = 9, \quad a_4 = 4(9) + 3(2) = 42$$

(d) $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$

Essa é uma relação de recorrência linear homogênea de terceira ordem com coeficientes constantes. Logo, precisamos de três, não duas, condições iniciais para termos uma única solução da relação de recorrência. Suponha que sejam dadas as condições iniciais $a_1 = 1, a_2 = 2, a_3 = 1$. Então os próximos elementos são os seguintes:

$$a_4 = 2(1) + 5(2) - 6(1) = 6, \quad a_5 = 2(2) + 5(1) - 6(6) = -37$$
$$a_6 = 2(1) + 5(6) - 6(-37) = 254$$

Este capítulo investiga as soluções de relações de recorrência lineares homogêneas com coeficientes constantes. A teoria de relações de recorrência não homogêneas e relações de recorrência sem coeficientes constantes está além do escopo deste texto.

Por conveniência computacional, a maioria de nossas sequências começará com a_0 em vez de a_1. A teoria não é afetada por isso.

6.8 RESOLVENDO RELAÇÕES DE RECORRÊNCIA LINEARES HOMOGÊNEAS DE SEGUNDA ORDEM

Considere uma relação de recorrência homogênea de segunda ordem com coeficientes constantes e que tem a forma

$$a_n = sa_{n-1} + ta_{n-2} \quad \text{ou} \quad a_n - sa_{n-1} - ta_{n-2} = 0$$

onde s e t são constantes com $t \neq 0$. Associamos o polinômio quadrático a seguir com a relação de recorrência acima.

$$\Delta(x) = x^2 - sx - t$$

Este polinômio $\Delta(x)$ é chamado de *polinômio característico* da relação de recorrência, e as raízes de $\Delta(x)$ são chamadas de *raízes características*.

Teorema 6.8: Suponha que o polinômio característico $\Delta(x) = x^2 - sx - t$ da relação de recorrência

$$a_n = sa_{n-1} + ta_{n-2}$$

tem raízes distintas r_1 e r_2. Então a solução geral da relação de recorrência, onde c_1 e c_2 são constantes arbitrárias é a seguinte:

$$a_n = c_1 r_1^n + c_2 r_2^n$$

Enfatizamos que as constantes c_1 e c_2 podem ser univocamente computadas usando condições iniciais. Observamos que o teorema é verdadeiro, mesmo quando as raízes não são reais. Tais casos estão fora do escopo deste livro.

Exemplo 6.10 Considere a relação de recorrência homogênea a seguir:

$$a_n = 2a_{n-1} + 3a_{n-2}$$

A solução geral é obtida primeiramente determinando o polinômio característico $\Delta(x)$ e suas raízes r_1 e r_2.

$$\Delta(x) = x^2 - 2x - 3 = (x-3)(x+1); \quad \text{raízes } r_1 = 3, r_2 = -1$$

Como as raízes são diferentes, podemos usar o Teorema 6.8 para obter a solução geral

$$a_n = c_1 3^n + c_2(-1)^n$$

Assim, quaisquer valores para c_1 e c_2 fornecem uma solução para a relação de recorrência.

Suponha que sejam dadas também as condições iniciais $a_0 = 1$, $a_1 = 2$. Usando a relação de recorrência, podemos calcular os próximos termos da sequência.

$$1, \quad 2, \quad 8, \quad 28, \quad 100, \quad 356, \quad 1268, \quad 3516, \ldots$$

A solução única é obtida encontrando c_1 e c_2 a partir das condições iniciais. Especificamente,

$$\text{Para } n = 0 \text{ e } a_0 = 1, \text{ temos } c_1 3^0 + c_2(-1)^0 = 1 \text{ ou } c_1 + c_2 = 1$$
$$\text{Para } n = 1 \text{ e } a_1 = 2, \text{ temos } c_1 3^1 + c_2(-1)^1 = 2 \text{ ou } 3c_1 - c_2 = 2$$

Resolvendo o sistema de duas equações relativamente às incógnitas c_1 e c_2, temos:

$$c_1 = \frac{3}{4} \quad \text{e} \quad c_2 = \frac{1}{4}$$

Assim, a solução a seguir da relação de recorrência dada é única, com as condições iniciais fornecidas $a_0 = 1$ e $a_1 = 2$.

$$a_n = \frac{3}{4}3^n + \frac{1}{4}(-1)^n = \frac{3^{n+1} + (-1)^n}{4}$$

Exemplo 6.11 Considere a célebre sequência de Fibonacci.

$$a_n = a_{n-1} + a_{n-2}, \quad \text{com} \quad a_0 = 0, a_1 = 1$$

Os 10 primeiros termos se seguem.

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Às vezes a sequência de Fibonacci é definida, usando as condições iniciais $a_0 = 1, a_1 = 1$ ou $a_1 = 1, a_2 = 2$. Empregamos $a_0 = 0, a_1 = 1$ por conveniência computacional. (As três condições iniciais fornecem a mesma sequência após o par de termos 1, 2.)

Observe que a sequência de Fibonacci é uma relação de recorrência linear homogênea de segunda ordem. Portanto, ela pode ser resolvida, usando o Teorema 6.8. Seu polinômio característico segue abaixo:

$$\Delta(x) = x^2 - x - 1$$

Usando a fórmula quadrática, obtemos as raízes:

$$r_1 = \frac{1+\sqrt{5}}{2} \qquad r_2 = \frac{1-\sqrt{5}}{2}$$

Pelo Teorema 6.8, obtemos a solução geral

$$a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$

As condições iniciais nos levam ao seguinte sistema de duas equações lineares em c_1 e c_2

Para $n = 0$ e $a_0 = 0$, temos $\quad 0 = c_1 + c_2$

Para $n = 1$ e $a_1 = 1$, temos $\quad 1 = c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right)$

A solução do sistema é como se segue:

$$c_1 = \frac{1}{\sqrt{5}}, \quad c_2 = -\frac{1}{\sqrt{5}}$$

Consequentemente, a seguir temos a solução da relação de recorrência de Fibonacci.

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Pode-se mostrar que o valor absoluto do segundo termo acima para a_n é sempre menor do que 1/2. Assim, a_n é também o inteiro mais próximo do número

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n \approx (0{,}4472)(1{,}6180)^n$$

Solução quando raízes do polinômio característico são iguais

Suponha que as raízes do polinômio característico não sejam distintas. Então temos o seguinte resultado.

Teorema 6.9: Considere que o polinômio característico $\Delta(x) = x^2 - sx - t$ da relação de recorrência

$$a_n = sa_{n-1} + ta_{n-2}$$

tem apenas uma raiz r_0. Então a solução geral da relação de recorrência, onde c_1 e c_2 são constantes arbitrárias é a seguinte:

$$a_n = c_1 r_0^n + c_2 n r_0^n$$

As constantes c_1 e c_2 podem ser calculadas univocamente, usando condições iniciais

Exemplo 6.12 Considere a seguinte relação de recorrência homogênea:

$$a_n = 6a_{n-1} - 9a_{n-2}$$

O polinômio característico $\Delta(x)$ é o que se segue:

$$\Delta(x) = x^2 - 6x + 9 = (x - 3)^2$$

Logo, $\Delta(x)$ tem apenas uma raiz $r_0 = 3$. Agora usamos o Teorema 6.9 para obter a seguinte solução geral da relação de recorrência.

$$a_n = c_1 3^n + c_2 n 3^n$$

Desse modo, quaisquer valores para c_1 e c_2 fornecem uma solução para a relação de recorrência.

Suponha que sejam dadas também as condições iniciais $a_1 = 3$, $a_2 = 27$. Utilizando a relação de recorrência podemos calcular os próximos termos da sequência:

$$3,\quad 27,\quad 135,\quad 567,\quad 2187,\quad 8109, \ldots$$

A solução única é obtida encontrando c_1 e c_2 a partir das condições iniciais. Especificamente

$$\text{Para } n = 1 \text{ e } a_1 = 3, \text{ temos } c_1 3^1 + c_2(1)(3)^1 = 3 \text{ ou } 3c_1 + 3c_2 = 3$$
$$\text{Para } n = 2 \text{ e } a_2 = 27, \text{ temos } c_1 3^2 + c_2(2)(3)^2 = 27 \text{ ou } 9c_1 + 18c_2 = 27$$

Resolvendo o sistema das duas equações relativamente às incógnitas c_1 e c_2, temos.

$$c_1 = -1 \text{ e } c_2 = 2$$

Logo, segue a solução única da relação de recorrência com as condições iniciais dadas.

$$a_n = -3^n + 2n3^n = 3^n(2n - 1)$$

6.9 RESOLVENDO RELAÇÕES DE RECORRÊNCIA LINEARES HOMOGÊNEAS GERAIS

Considere agora uma relação de recorrência linear homogênea de k-ésima ordem com coeficientes constantes que têm a forma

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + C_3 a_{n-3} + \cdots + C_k a_{n-k} = \sum_{i=1}^{k} C_i a_{n-i} \qquad (6.1)$$

onde $C_1, C_2, \ldots, C_k$ são constantes com $C_k \neq 0$. O *polinômio característico* $\Delta(x)$ da relação de recorrência (*6.1*) é o que se segue:

$$\Delta(x) = x^k - C_1 x^{k-1} - C_2 x^{k-2} - C_3 x^{k-3} - \cdots - C_k = x^k - \sum_{i=1}^{k} C_i x^{k-i}$$

As raízes de $\Delta(x)$ são chamadas de *raízes características* da relação de recorrência.

As seguintes observações são importantes.

Observação 1: Se $p(n)$ e $q(n)$ são soluções de (*6.1*), então qualquer combinação linear

$$c_1 p(n) + c_2 q(n)$$

de $p(n)$ e $q(n)$ também é uma solução. (Isso não é verdade se a relação de recorrência for não homogênea.)

Observação 2: Se r é uma raiz de multiplicidade m† do polinômio característico $\Delta(x)$ de *(6.1)*, então cada uma das seguintes

$$r^n, nr^n, n^2r^n, \ldots, n^{m-1}r^n$$

é uma solução de *(6.1)*. Assim, qualquer combinação linear

$$c_1r^n + c_2nr^n + c_3n^2r^n + \cdots + c_mn^{m-1}r^n = (c_1 + c_2n + c_3n^2 + \cdots + c_mn^{m-1})r^n$$

também é uma solução.

Exemplo 6.13 Considere a seguinte relação de recorrência homogênea de terceira ordem.

$$a_n = 11a_{n-1} - 39a_{n-2} + 45a_{n-3}$$

O polinômio característico $\Delta(x)$ da relação de recorrência é o que se segue:

$$\Delta(x) = x^3 - 11x^2 + 39x - 45 = (x-3)^2(x-5)$$

Logo, $\Delta(x)$ tem duas raízes, $r_1 = 3$ de multiplicidade 2 e $r_2 = 5$ de multiplicidade 1. Assim, de acordo com as observações acima, o que se segue é a solução geral da relação de recorrência.

$$a_n = c_1(3^n) + c_2n(3^n) + c_3(5^n) = (c_1 + c_2n)(3^n) + c_3(5^n)$$

Portanto, quaisquer valores para c_1, c_2 e c_3 fornecem uma solução para a relação de recorrência.

Suponha que sejam dadas também as condições iniciais $a_0 = 5$, $a_1 = 11$ e $a_2 = 25$. Usando a relação de recorrência, podemos calcular os próximos termos da sequência:

$$5, \quad 11, \quad 25, \quad 71, \quad 301, \quad 1667, \quad \ldots$$

A solução única é obtida encontrando c_1, c_2 e c_3 a partir das condições iniciais. Especificamente,

Para $n = 0$ e $a_0 = 5$, temos $c_1 + c_3 = 5$
Para $n = 1$ e $a_1 = 11$, temos $3c_1 + 3c_2 + 5c_3 = 11$
Para $n = 2$ e $a_2 = 25$, temos $9c_1 + 18c_2 + 25c_3 = 25$

Resolvendo o sistema de três equações relativamente às incógnitas c_1, c_2 e c_3, temos:

$$c_1 = 4, c_2 = -2 \text{ e } c_3 = 1$$

Portanto, o que se segue é a solução única da relação de recorrência com as condições iniciais dadas:

$$a_n = (4 - 2n)(3^n) + 5^n$$

Observação: Encontrar as raízes do polinômio característico $\Delta(x)$ é um passo importante para resolver relações de recorrência. Em termos gerais, isso pode ser difícil quando o grau de $\Delta(x)$ é maior do que 2. (O Exemplo B.16 no Apêndice B indica uma maneira para encontrar as raízes de alguns polinômios de grau 3 ou maior.)

Problemas Resolvidos

Técnicas avançadas de contagem, Inclusão-Exclusão

6.1 Uma panificadora vende $M = 5$ tipos de pães. Encontre o número m de maneiras que um cliente pode comprar: (*a*) 8 pães, (*b*) 12 pães.

† N. de T.: Tais raízes também podem ser referidas como duplas, triplas, quádruplas, etc.

Use $m = C(r + M - 1, r) = C(r + M - 1, M - 1)$, ou seja, o Teorema 6.1, uma vez que o problema se refere a combinações com repetições.

(*a*) Aqui $r = 8$ e, portanto, $m = C(8 + 4, 4) = C(12, 4) = 494$.

(*b*) Aqui $r = 12$ e, portanto, $m = C(12 + 4, 4) = C(16, 4) = 1820$

6.2 Encontre o número m de soluções não negativas para $x + y + z = 18$, com as condições de que $x \geq 3$, $y \geq 2$, $z \geq 1$.

Sejam $x' = x - 3$, $y' = y - 2$ e $z' = z - 1$. Então m é também o número de soluções não negativas de $x' + y' + z' = 12$. Como no Exemplo 6.1, esse segundo problema se refere a combinações com repetições, sendo $M = 3$ e $r = 12$. Logo,

$$m = C(12 + 2, 2) = C(14, 2) = 91.$$

6.3 Seja E a equação $x + y + z = 18$. Encontre o número m de soluções não negativas de E, com as condições de que $x < 7$, $y < 8$ e $z < 9$.

Seja S o conjunto de todas as soluções não negativas de E. Sejam A o conjunto de soluções para as quais $x \geq 7$, B o conjunto de soluções tais que $y \geq 8$, e C o conjunto de soluções para as quais $z \geq 9$. Então,

$$m = |A^C \cap B^C \cap C^C|$$

Como no Problema 6.1, obtemos

$$\begin{aligned} |A| &= C(11 + 2, 2) = 78, & |A \cap B| &= C(3 + 2, 2) = 10 \\ |B| &= C(10 + 2, 2) = 66, & |A \cap C| &= C(2 + 2, 2) = 6 \\ |C| &= C(9 + 2, 2) = 55, & |B \cap C| &= C(1 + 2, 2) = 3 \end{aligned}$$

Além disso, $|S| = C(18 + 2, 2) = 190$ e $|A \cap B \cap C| = 0$. Pelo Princípio de Inclusão-Exclusão,

$$m = 190 - (78 + 66 + 55) + (10 + 6 + 3) - 0 = 10$$

6.4 Há 9 alunos em uma turma. Encontre o número m de maneiras que: (*a*) os 9 alunos podem fazer 3 testes diferentes se 3 estudantes realizam cada teste; (*b*) os 9 alunos podem ser particionados em 3 equipes A, B e C, de forma que cada equipe contém 3 estudantes.

(*a*) Método 1 Procuramos pelo número m de partições dos 9 alunos em células contendo 3. Pelo Teorema 6.2, $m = 9!/(3!3!3!) = 5040$.

Método 2 Existem $C(9, 3)$ maneiras para escolher três alunos para realizarem o primeiro teste; em seguida há $C(6, 3)$ maneiras para escolher três alunos para realizarem o segundo teste, e os demais alunos fazem o terceiro teste. Logo, $m = C(9, 3)C(6, 3) = 5040$.

(*b*) Cada partição $\{A, B, C\}$ dos alunos pode ser arranjada de $3! = 6$ maneiras como uma partição ordenada. De acordo com (*a*), existem 5040 partições desse tipo. Logo, $m = 5040/6 = 840$.

6.5 Encontre o número N de maneiras que uma companhia pode designar 7 projetos para 4 pessoas, de modo que cada pessoa assume pelo menos um projeto.

Queremos encontrar o número N de funções sobrejetoras de um conjunto com $m = 7$ elementos em um conjunto com $n = 4$ elementos. Usamos o Teorema 6.4

$$\begin{aligned} N &= 4^7 - C(4, 1)(3^7) + C(4, 2)(2^7) - C(4, 3)(1^7) \\ &= 4^7 - 4(3^7) + 6(2^7) - 4(1^7) = 16\,384 - 8748 + 768 - 4 = 8400 \end{aligned}$$

6.6 Demonstre o Teorema 6.5: $D_n = n![1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}]$

Lembre que (Seção 3.3) S_n denota o conjunto de permutações sobre $X = \{1, 2, \ldots, n\}$ e $|S_n| = n!$. Para $i = 1, \ldots, n$, seja F_i todas as permutações em S_n que "fixam i", ou seja, $F_i = \{\sigma \in S_n \mid \sigma(i) = i\}$. Então, para subscritos distintos,

$$|F_i| = (n - 1)!, \; |F_i \cap F_j| = (n - 2)!, \; \ldots, \; |F_{i_1} \cap F_{i_2} \cap \cdots \cap F_{i_r}| = (n - r)!$$

Seja Y o conjunto de todos os desarranjos em S_n. Então

$$D_n = |Y| = |F_1^C \cap F_2^C \cap \cdots \cap F_n^C|$$

Pelo Princípio de Inclusão-Exclusão,

$$D_n = |S_n| - s_1 + s_2 - s_3 + \cdots + (-1)^n s_n$$

onde

$$s_r = \sum_{i_1 < i_2 < \cdots < i_r} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_r}| = C(n, r)(n - r)! = \frac{n!}{r!}$$

Fazendo $|S_n| = n!$ e $s_r = n!/r!$ na fórmula para D_n, temos nosso teorema.

Princípio da Casa dos Pombos

6.7 Suponha que cinco pontos são escolhidos no interior de um quadrado S, onde cada lado tem comprimento de duas polegadas. Mostre que a distância entre dois dos pontos deve ser menor do que $\sqrt{2}$ polegadas.

Esboce dois segmentos de reta entre os lados opostos de S que particione S em quatro subquadrados, cada um tendo lados de uma polegada. Pelo Princípio da Casa dos Pombos, dois dos pontos estão em um dos subquadrados. A diagonal de cada subquadrado mede $\sqrt{2}$ polegadas. Logo, a distância entre os dois pontos é menor do que $\sqrt{2}$ polegadas.

6.8 Sejam p e q inteiros positivos. Um número r é dito satisfazer a propriedade (p, q)-Ramsey se um conjunto de r pessoas deve ter um subconjunto de p amigos mútuos ou um subconjunto de q desconhecidos mútuos. O número de Ramsey $R(p, q)$ é o menor inteiro r que satisfaz isso. Mostre que $R(3, 3) = 6$.

Pelo Exemplo 6.5, $R(3, 3) \geq 6$. Mostramos que $R(3, 3) > 5$. Considere cinco pessoas que sentam ao redor de uma mesa redonda, e suponha que cada pessoa é amiga apenas de quem está sentado ao lado dela. Não podem haver três desconhecidos entre si, uma vez que duas das três pessoas devem estar sentadas uma ao lado da outra. Além disso, três pessoas não podem ser amigas mútuas, pois elas não podem estar sentadas uma ao lado da outra. Logo, $R(3, 3) > 5$. Consequentemente, $R(3, 3) = 6$.

6.9 Suponha que um time disputa 18 jogos em um período de 14 dias seguidos, e participa de pelo menos um jogo por dia. Mostre que há um período de dias no qual exatamente 9 jogos foram disputados.

Seja $S = \{s_1, s_2, \ldots, s_{14}\}$, onde s_i é o número de jogos X disputados do primeiro ao i-ésimo dia. Então, $s_{14} = 18$, e todos os s_i são distintos. Seja $T = \{t_1, t_2, \ldots, t_{14}\}$, onde $t_i = s_i + 9$. Então, $t_{14} = 18 + 9 = 27$, e os t_i são distintos. Juntos, S e T têm $14 + 14 = 28$ números que ficam entre 1 e 27. Pelo Princípio da Casa dos Pombos, dois dos números devem ser iguais. Contudo, as entradas em S e as entradas em T são diferentes. Assim, há $s_j \in S$ e $t_k \in T$ tais que $s_j = t_k = s_k + 9$. Portanto,

$$9 = s_j - s_k = \text{número de jogos disputados nos dias } k + 1, k + 2, \ldots, j - 1, j$$

6.10 Prove o Teorema 6.7. Toda sequência com $n^2 + 1$ números reais distintos contém uma subsequência de comprimento $n + 1$ que é estritamente crescente ou estritamente decrescente.

Seja $a_1, a_2, \ldots, a_{n^2+1}$ uma sequência de $n^2 + 1$ números reais diferentes. Para cada a_i podemos associar o par (i_i, d_i), onde (1) i_i é a mais longa subsequência crescente começando em a_i e (2) d_i é a mais longa subsequência decrescente começando em a_i. Assim, há $n^2 + 1$ pares ordenados desse tipo, um para cada número na sequência.

Agora suponha que nenhuma subsequência é mais longa do que n. Então, i_i e d_i não podem exceder n. Logo, há no máximo n^2 pares distintos (i_i, d_i). Pelo Princípio da Casa dos Pombos, dois dos $n^2 + 1$ pares são iguais, ou seja, há dois pontos distintos a_r e a_s tais que $(i_r, d_r) = (i_s, d_s)$. Sem perda de generalidade, podemos assumir que $r < s$. Então, a_r ocorre antes de a_s na sequência (Ver Fig. 6-2(a)). Portanto, a_r seguido pela subsequência crescente de i_s números começando em a_s nos dá uma subsequência de comprimento $i_s + 1 = i_r + 1$ iniciando em a_r (Ver Fig. 6-2(b)). Isso contradiz a definição de i_r. Analogamente, suponha que $a_r > a_s$. Então, a_r seguido pela subsequência decrescente de d_s números começando em a_s nos dá uma subsequência de comprimento $d_r + 1 = d_s + 1$ iniciando em a_r, o que contradiz a definição de d_r (Ver Fig. 6-2(c)). Em cada caso conseguimos uma contradição. Logo, a hipótese de que nenhuma subsequência excede n é falsa, e o teorema está demonstrado.

Figura 6-2

Recursão

6.11 Considere a relação de recorrência homogênea de segunda ordem $a_n = a_{n-1} + 2a_{n-2}$, com condições iniciais $a_0 = 2$, $a_1 = 7$

(*a*) Encontre os próximos três termos da sequência.

(*b*) Encontre a solução geral.

(*c*) Encontre a solução única, com as condições iniciais dadas.

(*a*) Cada termo é a soma do termo anterior com o dobro do termo que imediatamente antecede este anterior. Assim.

$$a_2 = 7 + 2(2) = 11,\ a_3 = 11 + 2(7) = 25,\ a_4 = 25 + 2(11) = 46$$

(*b*) Primeiro encontramos o polinômio característico $\Delta(t)$ e suas raízes:

$$\Delta(x) = x^2 - x - 2 = (x - 2)(x + 1);\ \text{raízes } r_1 = 2,\ r_2 = -1$$

Como as raízes são distintas, usamos o Teorema 6.8 para obter a solução geral.

$$a_n = c_1(2^n) + c_2(-1)^n$$

(c) A solução única é obtida encontrando c_1 e c_2 a partir das condições iniciais

$$\begin{array}{lll} \text{Para } n = 0,\ a_0 = 2, & \text{temos} & c_1(2^0) + c_2(-1)^0 = 2 \text{ ou } c_1 + c_2 = 2 \\ \text{Para } n = 1,\ a_1 = 7, & \text{temos} & c_1(2^1) + c_2(-1)^1 = 7 \text{ ou } 2c_1 - c_2 = 7 \end{array}$$

Resolvendo as duas equações relativamente a c_1 e c_2, temos $c_1 = 3$ e $c_2 = 1$. A solução única é a que se segue:

$$a_n = 3(2^n) - (-1)^n$$

6.12 Considere a relação de recorrência homogênea de terceira ordem $a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3}$.

(*a*) Encontre a solução geral.

(*b*) Encontre a solução, com condições iniciais $a_0 = 3$, $a_1 = 4$, $a_2 = 12$.

(*a*) Primeiro determinamos o polinômio característico

$$\Delta(x) = x^3 - 6x^2 + 12x - 8 = (x - 2)^3$$

Então $\Delta(x)$ tem apenas uma raiz $r_0 = 2$ de multiplicidade 3. Assim, a solução geral da relação de recorrência é a que se segue.

$$a_n = c_1(2^n) + c_2n(2^n) + c_3n^2(2^n) = (c_1 + c_2n + c_3n^2)(2^n)$$

(*b*) Determinamos os valores de c_1, c_2 e c_3 como se segue:

$$\begin{array}{lll} \text{Para } n = 0,\ a_0 = 3, & \text{temos} & c_1 = 3 \\ \text{Para } n = 1,\ a_1 = 4, & \text{temos} & 2c_1 + 2c_2 + 2c_3 = 4 \\ \text{Para } n = 2,\ a_2 = 12, & \text{temos} & 4c_1 + 8c_2 + 16c_3 = 12 \end{array}$$

Resolvendo o sistema de três equações relativamente a c_1, c_2 e c_3, temos a solução

$$c_1 = 3,\ c_2 = -2,\ c_3 = 1$$

Logo, a solução única da relação de recorrência é a seguinte:

$$a_n = (3 - 2n + n^2)(2^n)$$

Problemas Complementares

Técnicas avançadas de contagem, inclusão-exclusão

6.13 Uma loja vende $M = 4$ tipos de biscoitos. Encontre o número de maneiras que um cliente pode comprar

(a) 10 biscoitos; (b) 15 biscoitos.

6.14 Encontre o número m de soluções não negativas para $x + y + z = 20$, com as condições de que $x > 5$, $y > 3$ e $z > 1$

6.15 Seja E a equação $x + y + z = 20$. Encontre o número de soluções não negativas para E, com as condições de que $x < 8$, $y < 9$ e $z < 10$.

6.16 Encontre o número m de inteiros positivos que não excedem 1000 e que não são divisíveis por 3, 7 ou 11.

6.17 Encontre o número de maneiras que 14 pessoas podem ser particionadas em 6 comitês, de modo que 2 comitês contêm três pessoas e os outros, duas.

6.18 Assuma que uma célula pode ser vazia. Encontre o número m de maneiras que um conjunto:

(a) De três pessoas pode ser particionado em: (i) três células ordenadas, (ii) três células não ordenadas.

(b) De quatro pessoas pode ser particionado em: (i) três células ordenadas, (ii) três células não ordenadas.

6.19 Encontre o número N de funções sobrejetoras de um conjunto A em um conjunto B, onde:

(a) $|A| = 8$, $|B| = 3$; (b) $|A| = 6$, $|B| = 4$, (c) $|A| = 5$, $|B| = 5$, (d) $|A| = 5$, $|B| = 7$

6.20 Encontre o número de desarranjos de $X = \{1, 2, 3, \ldots, 2m\}$ tal que os primeiros m elementos de cada desarranjo são (a) os primeiros m elementos de X; (b) os últimos m elementos de X.

Princípio da Casa dos Pombos

6.21 Encontre o número mínimo de estudantes que podem ser matriculados em uma faculdade, de modo que exista pelo menos 13 estudantes de cada um dos 50 estados.†

6.22 Considere nove pontos reticulados no espaço. Mostre que o ponto médio de dois desses pontos é também um ponto reticulado.

6.23 Encontre uma subsequência crescente de comprimento máximo e uma subsequência decrescente de comprimento máximo na sequência 14, 2, 8, 3, 25, 15, 10, 20, 9, 4.

6.24 Considere uma fila de 50 pessoas com alturas distintas. Mostre que há uma subfila de 8 pessoas cujas alturas estão aumentando ou diminuindo.

6.25 Dê um exemplo de uma sequência de 25 inteiros diferentes a qual não admite uma subsequência de 6 inteiros que está aumentando ou diminuindo.

6.26 Suponha que uma equipe X disputa 19 jogos em um período de 14 dias seguidos, e participa de pelo menos um jogo por dia. Mostre que há um período de dias corridos em que X disputou exatamente 8 jogos.

6.27 Suponha que 10 pontos foram escolhidos ao acaso no interior de um triângulo equilátero T, onde cada lado tem comprimento de três polegadas. Mostre que a distância entre dois dos pontos deve ser menor do que uma polegada.

6.28 Seja $X = \{x_i\}$ um conjunto de n inteiros positivos. Mostre que a soma dos inteiros de um subconjunto de X é divisível por n.

6.29 Considera um grupo de 10 pessoas (onde cada par é de amigos ou desconhecidos). Mostre que há um subgrupo de quatro amigos mútuos ou um subgrupo de três desconhecidos mútuos.

6.30 Para os números de Ramsey $R(p, q)$ mostre que: (a) $R(p, q) = R(q, p)$; (b) $R(p, 1) = 1$, (c) $R(p, 2) = p$.

Recursão

6.31 Para cada relação de recorrência e conjunto de condições iniciais, encontre: (i) a solução geral; (ii) a solução única, com as condições iniciais dadas.

(a) $a_n = 3a_{n-1} + 10a_{n-2}$, $a_0 = 5$, $a_1 = 11$ (d) $a_n = 5a_{n-1} - 6a_{n-2}$, $a_0 = 2$, $a_1 = 8$

(b) $a_n = 4a_{n-1} + 21a_{n-2}$, $a_0 = 9$, $a_1 = 13$ (e) $a_n = 3a_{n-1} - a_{n-2}$, $a_0 = 0$, $a_1 = 1$

(c) $a_n = 3a_{n-1} - 2a_{n-2}$, $a_0 = 5$, $a_1 = 8$ (f) $a_n = 5a_{n-1} - 3a_{n-2}$, $a_0 = 0$, $a_1 = 1$

6.32 Repita o problema 6.31 para as seguintes relações de recorrência e condições iniciais.

(a) $a_n = 6a_{n-1}$; $a_0 = 5$ (c) $a_n = 4a_{n-1} - 4a_{n-2}$; $a_0 = 1$, $a_1 = 8$

(b) $a_n = 7a_{n-1}$; $a_0 = 5$ (d) $a_n = 10a_{n-1} - 25a_{n-2}$; $a_0 = 2$, $a_1 = 15$

---

† N. de T.: Os autores se referem aos estados dos Estados Unidos.

6.33 Encontre a solução única para cada relação de recorrência, com as condições iniciais dadas:

(a) $a_n = 10a_{n-1} - 32a_{n-2} + 32a_{n-3}$ com $a_0 = 5, a_1 = 18, a_2 = 76$

(b) $a_n = 9a_{n-1} - 27a_{n-2} + 27a_{n-3}$ com $a_0 = 5, a_1 = 24, a_2 = 117$

6.34 Considere a seguinte relação de recorrência de segunda ordem e seu polinômio característico $\Delta(x)$:

$$a_n = sa_{n-1} + ta_{n-2} \text{ e } \Delta(x) = x^2 - sx - t \qquad (*)$$

(a) Suponha que $p(n)$ e $q(n)$ são soluções de $(*)$. Mostre que, para quaisquer constantes c_1 e c_2, $c_1p(n) + c_2q(n)$ também é uma solução de $(*)$.

(b) Suponha que r é uma raiz de $\Delta(x)$. Mostre que $a_n = r^n$ é uma solução de $(*)$.

(c) Suponha que r é uma raiz dupla de $\Delta(x)$. Mostre que: (i) $s = 2r$ e $t = -r^2$, (ii) $a_n = nr^n$ também é uma raiz de $(*)$.

6.35 Repita o Problema 6.34(a) e (b) para qualquer relação de recorrência homogênea linear de k-ésima ordem com coeficientes constantes e polinômio característico $\Delta(x)$ dados por

$$a_n = C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} = \sum_{i=1}^{k} C_ia_{n-i} \quad \text{e} \quad \Delta(x) = x^k - \sum_{i=1}^{k} C_ix^{k-i}$$

Respostas dos Problemas Complementares

6.13 (a) 286, (b) 646.

6.14 78

6.15 15.

6.16 520.

6.17 (14!)/[(3!3!2!2!2!2!)(2!4!)] = 3 153 150.

6.18 (a) (i) $3^3 = 27$; (ii) Elas podem ser distribuídas como: [3, 0, 0], [2, 1, 0] ou [1, 1, 1]. Logo, $m = 1 + 3 + 1 = 5$. (b) (i) $3^4 = 81$; (ii) Elas podem ser distribuídas como: [4, 0, 0], [3, 1, 0], [2, 2, 0] ou [2, 1, 1]. Logo, $m = 1 + 4 + 3 + 6 = 14$.

6.19 (a) 5796; (b) 1560; (c) $5! = 120$; (d) 0.

6.20 (a) $(D_m)^2$; (b) $(m!)^2$.

6.21 701

6.22 Há oito triplas de paridades: (ímpar, ímpar, ímpar), (ímpar, ímpar, par), ... Assim, dois dos nove pontos têm a mesma tripla de paridades.

6.23 2, 3, 10, 20; 25, 15, 10, 8, 4.

6.24 Use o Teorema 6.7 com $n = 9$.

6.25 5, 4, 3, 2, 1, 10, 9, 8, 7, 6, ..., 25, 24, 23, 22, 21.

6.26 (Sugestão: Veja o Problema 6.9.)

6.27 (Sugestão: Particione T em 9 triângulos equiláteros, onde cada lado tem comprimento de uma polegada.)

6.28 Seja $s_i = x_1 + \cdots + x_i$. O resultado é verdadeiro se n divide algum s_i. Caso contrário, seja r_i o resto, quando s_i é dividido por n. Dois dos r's devem ser iguais. Digamos, $r_p = r_q$, onde $p < q$. Então n divide $s_p - s_q = x_{p+1} + \cdots + x_q$.

6.31 (a) $a_n = c_1(5^n) + c_2(-2)^n$, $c_1 = 3, c_2 = 2$

(b) $a_n = c_1(7^n) + c_2(-3)^n$, $c_1 = 4, c_2 = 5$

(c) $a_n = c_1 + c_2(2^n)$; $c_1 = 2, c_2 = 3$

(d) $a_n = c_1(2^n) + c_2(3)^n$, $c_1 = -2, c_2 = 4$

(e) $a_n = c_1[(3 + t)/2]^n + c_2[(3 - t)/2]^n$; $c_1 = 1/t$, $c_2 = -1/t$, onde $t = \sqrt{5}$.

(f) $a_n = c_1[(5 + s)/2]^n + c_2[(5 - s)/2]^n$; $c_1 = 1/s$, $c_2 = -1/s$, onde $s = \sqrt{13}$.

6.32 (a) $a_n = c_1(6^n)$, $c_1 = 5$

(b) $a_n = c_1(7^n)$, $c_1 = 5$

(c) $a_n = c_1(2^n) + c_2n(2^n)$, $c_1 = 1, c_2 = 3$

(d) $a_n = c_1(5^n) + c_2n(5^n)$, $c_1 = 2, c_2 = 1$

6.33 (a) $a_n = 2(4^n) + n(4^n) + 3(2^n)$; (b) $a_n = 5(3^n) + 2n(3^n) + n^2(3^n) = (5 + 2n + n^2)3^n$

6.34 (b) r é uma raiz de $\Delta(x)$. Logo, $r^2 - sr - t = 0$ ou $r^2 = sr + t$. Seja $a_n = r^n$. Então, $sa_{n-1} + ta_{n-2} = sr^{n-1} + tr^{n-2} = (sr + t)r^{n-2} = r^2(r^{n-2}) = r^n = a_n$.

(c) (i) r é uma raiz dupla de $\Delta(x)$; logo, $\Delta(x) = (x - r)^2 = x^2 - 2rx + r^2 = x^2 - sx - t$. Assim, $s = 2r$ e $t = -r^2$. (ii) Seja $a_n = nr^n$. Então, $sa_{n-1} + ta_{n-2} = \cdots = nr^n = a_n$.

Probabilidade

7.1 INTRODUÇÃO

Teoria de probabilidade é um modelo matemático dos fenômenos de acaso ou aleatoriedade. Se uma moeda é jogada de uma maneira aleatória, pode resultar em cara ou coroa, mas não sabemos qual dessas possibilidades ocorrerá em uma única jogada. Contudo, suponha que consideremos s o número de vezes que aparecem caras quando a moeda é jogada n vezes. À medida que n aumenta, a razão $f = s/n$, chamada de *frequência relativa* do resultado, se torna mais estável. Se a moeda é não viciada, então esperamos que ela resulte em cara aproximadamente 50% das vezes ou, em outras palavras, a frequência relativa se aproxima de $\frac{1}{2}$. Além disso, assumindo que a moeda tem massa perfeitamente distribuída, podemos obter o valor $\frac{1}{2}$ por meios dedutivos. Isto é, qualquer lado da moeda é tão provável de ocorrer quanto o outro; logo, as chances de obter cara é de uma em duas, o que significa que a probabilidade de obter cara é $\frac{1}{2}$. Apesar de o resultado específico de qualquer jogada ser desconhecido, o comportamento ao longo de muitas jogadas é determinado. Esse comportamento estável de longo termo de fenômenos aleatórios forma a base da teoria de probabilidades.

Um modelo matemático probabilístico de fenômenos aleatórios é definido associando "probabilidades" a todos os possíveis resultados de um experimento. A confiabilidade de nosso modelo matemático para um dado experimento depende da proximidade das probabilidades associadas com o limite das frequências relativas. Isso dá origem a problemas de teste e confiabilidade, que constituem um tema da estatística e estão além do escopo deste livro.

7.2 ESPAÇO AMOSTRAL E EVENTOS

O conjunto S de todos os possíveis resultados de um dado experimento é chamado de *espaço amostral*. Um resultado específico, ou seja, um elemento de S, é chamado de *ponto amostral*. Um *evento* A é um conjunto de resultados ou, em outras palavras, um subconjunto do espaço amostral S. Em particular, o conjunto $\{a\}$ consistindo em um único ponto amostral $a \in S$ é chamado de *evento elementar*. Além disso, o conjunto vazio e o próprio $\varnothing$ são subconjuntos de S e, assim, $\varnothing$ e S também são eventos. $\varnothing$ é, às vezes, chamado de *evento impossível* ou *evento nulo*.

Como um evento é um conjunto, podemos combinar eventos para formar novos, usando as várias operações conjuntistas:†

(i) $A \cup B$ é o evento que ocorre se, e somente se, A *ou* B ocorrem (ou ambos).

(ii) $A \cap B$ é o evento que ocorre se, e somente se, A *e* B ocorrem.

(iii) A^c, o complementar de A, também escrito $\overline{A}$, é o evento que ocorre se, e somente se, A *não* ocorre.

Dois eventos A e B são chamados de *mutuamente exclusivos* se forem disjuntos, ou seja, se $A \cap B = \varnothing$. Em outras palavras, A e B são mutuamente exclusivos se, e somente se, eles não puderem ocorrer simultaneamente. Três ou mais eventos são mutuamente exclusivos se cada par deles forem mutuamente exclusivos.

† N. de T.: Muitos livros sobre probabilidades se referem a essa álgebra conjuntista de eventos como σ-álgebra (sigma álgebra).

Exemplo 7.1

(a) ***Experimento:*** Jogue uma moeda três vezes e observe a sequência de caras (A) e coroas (O) que aparece.

O espaço amostral consiste nos oito elementos a seguir:

$$S = \{AAA, AAO, AOA, AOO, OAA, OAO, OOA, OOO\}$$

Seja A o evento de que duas ou mais caras aparecem consecutivamente, e B o evento de que todos os resultados são o mesmo:

$$A = \{AAA, AAO, OAA\} \text{ e } B = \{AAA, OOO\}$$

Então $A \cap B = \{AAA\}$ é o evento elementar de que apenas caras aparecem. O evento de que cinco caras aparecem é o conjunto vazio $\varnothing$.

(b) ***Experimento:*** Jogue um dado (de seis faces), representado na Fig. 7-1(a), e observe o número (de pontos) que surge no topo.

O espaço amostral consiste nos seis possíveis números, isto é, $S = \{1, 2, 3, 4, 5, 6\}$. Seja A o evento de que um número par apareça, B o evento de que um número ímpar apareça, e C o evento de que um número primo apareça. Isto é,

$$A = \{2, 4, 6\}, B = \{1, 3, 5\}, C = \{2, 3, 5\}$$

Então

$A \cup C = \{2, 3, 4, 5, 6\}$ é o evento de que um número par ou primo ocorra.

$B \cap C = \{3, 5\}$ é o evento de que um número ímpar e primo ocorra.

$C^c = \{1, 4, 6\}$ é o evento de que um número primo não ocorra.

Observe que A e B são mutuamente exclusivos. $A \cap B = \varnothing$. Em outras palavras, um número par e um número ímpar não podem ocorrer simultaneamente.

(c) ***Experimento:*** Jogue uma moeda até uma cara aparecer, e conte o número de vezes que a moeda foi jogada.

O espaço amostral S desse experimento é $S = \{1, 2, 3, \ldots\}$. Como todo inteiro positivo é um elemento de S, o espaço amostral é infinito.

Observação: O espaço amostral S do Exemplo 7.1(c), como observado, não é finito. A teoria referente a tais espaços amostrais está além do escopo deste texto. Assim, a não ser que seja dito o contrário, todos os nossos espaços amostrais S são finitos.

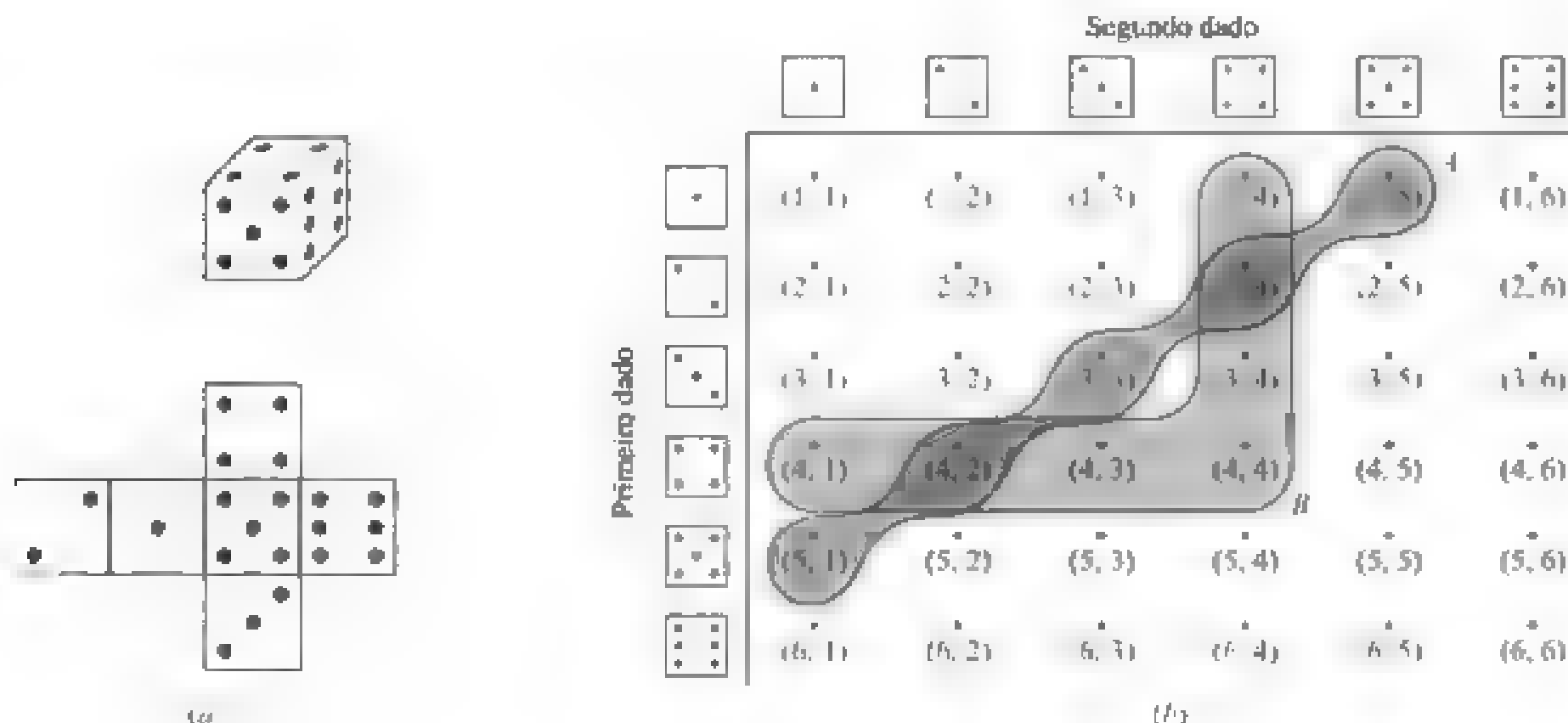



Figura 7-1

***Exemplo 7.2* (Par de dados)** Jogue um par de dados e registre os dois números no topo.

Há seis possíveis números, 1, 2, ..., 6, em cada dado. Logo, S consiste nos pares de números de 1 a 6 e, consequentemente, $n(S) = 36$. A Fig. 7-1(b) mostra esses 36 pares de números arranjados em uma tabela onde as linhas são rotuladas pelo primeiro dado e as colunas pelo segundo dado.

Seja A o evento no qual a soma dos dois números é 6, e seja B o evento no qual o maior dos dois números é 4. Isto é,

$$A = \{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\}, B = \{(1, 4), (2, 4), (3, 4), (4, 4), (4, 3), (4, 2), (4, 1)\}$$

Então o evento "A e B" consiste nos pares de inteiros cuja soma é 6 e nos quais o maior número é 4 ou, em outras palavras, trata-se da interseção entre A e B. Assim,

$$A \cap B = \{(2, 4), (4, 2)\}$$

Analogamente, em "A ou B", a soma é 6 ou o maior número é 4, sombreado na Fig. 7-1(b), o que corresponde à união $A \cup B$.

***Exemplo 7.3* (Baralho de cartas)** Uma carta é retirada de um baralho comum de 52 cartas, representado na Fig. 7-2(a).

O espaço amostral S consiste nos quatro *naipes*, paus (P), ouro (O), copas (C) e espadas (E), onde cada naipe contém 13 cartas numeradas de 2 a 10, valete (J), rainha (Q), rei (K) e ás (A). As cartas de copas (C) e de ouro (O) são vermelhas, de espadas (E) e de paus (P) são pretas. A Fig. 7-2(b) retrata 52 pontos que correspondem ao baralho S da maneira óbvia. Seja E o evento de uma *carta pictórica*, ou *de rosto*, isto é, um valete (J), uma rainha (Q) ou um rei (K), e seja F o evento de uma carta de copas. Então $E \cap F = \{JC, QC, KC\}$, como sombreado na Fig. 7-2(b).

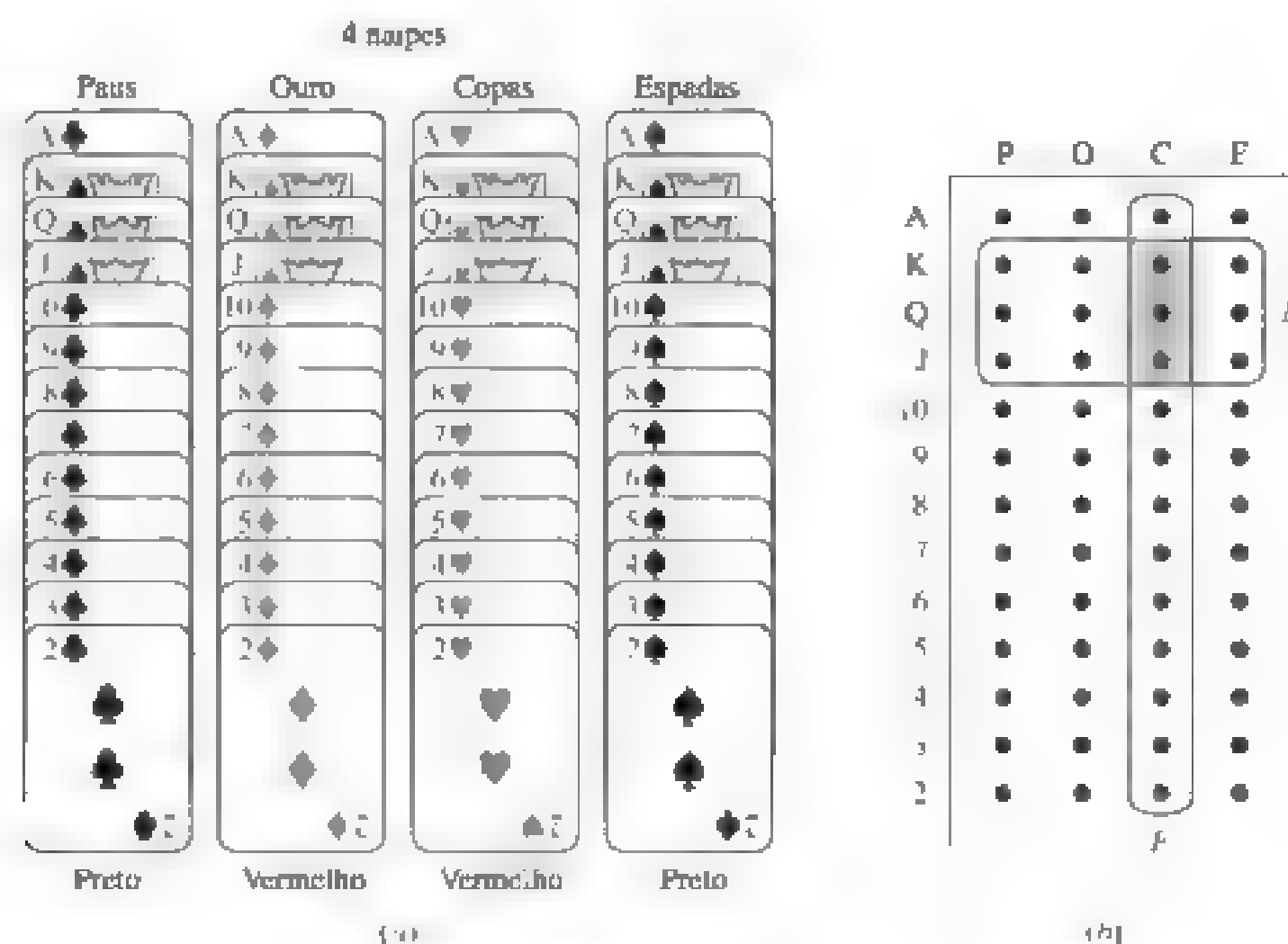



Figura 7-2

7.3 ESPAÇOS FINITOS DE PROBABILIDADES

A seguinte definição se aplica.

Definição 7.1: Seja S um espaço amostral finito, digamos, $S = \{a_1, a_2, \ldots, a_n\}$. Um *espaço finito de probabilidades*, ou *modelo probabilístico*, é obtido correspondendo a cada ponto a_i em S um número real p_i, dito a *probabilidade* de a_i, satisfazendo às seguintes propriedades.

(i) Cada p_i é não negativo, isto é, $p_i \geq 0$.
(ii) A soma dos p_i é 1, ou seja, $p_1 + p_2 + \cdots + p_n = 1$.

A *probabilidade* de um evento A, denotada por $P(A)$, é então definida como a soma das probabilidades dos pontos em A. O conjunto unitário $\{a_i\}$ é chamado de evento *elementar* e, por conveniência de notação, escrevemos $p(a_i)$ no lugar de $p(\{a_i\})$.

***Exemplo 7.4* (Experimento)** Suponha que três moedas são jogadas e que o número de caras é registrado. (Compare com o Exemplo 7.1(a).)

O espaço amostral é $S = \{0, 1, 2, 3\}$. As seguintes correspondências sobre os elementos de S definem um espaço de probabilidades.

$$P(0) = \tfrac{1}{8}, P(1) = \tfrac{3}{8}, P(2) = \tfrac{3}{8}, P(3) = \tfrac{1}{8}$$

Ou seja, cada probabilidade é não negativa e a soma das probabilidades é 1. Seja A o evento de que pelo menos uma cara aparece, e seja B o evento de que todas as caras e todas as coroas aparecem, ou seja, $A = \{1, 2, 3\}$ e $B = \{0, 3\}$. Então, por definição,

$$P(A) = P(1) + P(2) + P(3) = \tfrac{3}{8} + \tfrac{3}{8} + \tfrac{1}{8} = \tfrac{7}{8} \text{ e } P(B) = P(0) + P(3) = \tfrac{1}{8} + \tfrac{1}{8} = \tfrac{1}{4}$$

Espaços equiprováveis

Frequentemente, as características físicas de um evento sugerem que os vários resultados do espaço amostral sejam correspondidos a probabilidades idênticas. Tal espaço finito de probabilidades S, onde cada ponto amostral tem a mesma probabilidade, é chamado de *espaço equiprovável*. Em particular, se S contém n pontos, então a probabilidade de cada ponto é $1/n$. Além disso, se um evento A contém r pontos, então sua probabilidade é $r(1/n) = r/n$. Vale notar que $n(A)$ denota o número de elementos de um conjunto A

$$P(A) = \frac{\text{número de elementos em } A}{\text{número de elementos em } S} = \frac{n(A)}{n(S)} \quad \text{ou} \quad P(A) = \frac{\text{número de resultados favoráveis a } A}{\text{número total de possíveis resultados}}$$

Enfatizamos que a fórmula acima para $P(A)$ somente pode ser usada em um espaço equiprovável e não pode ser empregada indiscriminadamente.

A expressão *aleatoriamente* é utilizada apenas em espaços equiprováveis, a afirmação "escolha um ponto aleatoriamente de um conjunto S" significa que todo ponto de S tem a mesma probabilidade de ser escolhido.

Exemplo 7.5 Seja uma carta escolhida de um baralho comum de 52 cartas. Sejam

$$A = \{\text{a carta é de espadas}\} \text{ e } B = \{\text{a carta é pictórica}\}$$

Calculamos $P(A)$, $P(B)$ e $P(A \cap B)$. Uma vez que temos uma espaço equiprovável,

$$P(A) = \frac{\text{número de cartas de espadas}}{\text{número de cartas}} = \frac{13}{52} = \frac{1}{4}, \quad P(B) = \frac{\text{número de cartas pictóricas}}{\text{número de cartas}} = \frac{12}{52} = \frac{3}{13}$$

$$P(A \cap B) = \frac{\text{número de cartas pictóricas de espadas}}{\text{número de cartas}} = \frac{3}{52}$$

Teoremas sobre espaços finitos de probabilidades

O teorema a seguir é consequência direta do fato de que a probabilidade de um evento é a soma das probabilidades de seus pontos.

Teorema 7.1: A função de probabilidade P definida sobre a classe de todos os eventos de um espaço finito de probabilidades tem as seguintes propriedades:

> $[\mathbf{P}_1]$ Para todo evento A, $0 \leq P(A) \leq 1$.
> $[\mathbf{P}_2]$ $P(S) = 1$.
> $[\mathbf{P}_3]$ Se eventos A e B são mutuamente exclusivos, então $P(A \cup B) = P(A) + P(B)$.

O próximo teorema formaliza nossa intuição de que se p é a probabilidade de que um evento ocorra, então $1 - p$ é a probabilidade de que E não ocorra. (Ou seja, se atingimos um alvo $p = 1/3$ das vezes, então erramos o alvo $1 - p = 2/3$ das vezes.)

Teorema 7.2: Seja A um evento qualquer. Então $P(A^C) = 1 - P(A)$.

O teorema a seguir (demonstrado no Problema 7.13) deriva diretamente do Teorema 7.1.

Teorema 7.3: Considere o conjunto vazio $\varnothing$ e quaisquer eventos A e B. Então:

(i) $P(\varnothing) = 0$.
(ii) $P(A \backslash B) = P(A) - P(A \cap B)$.
(iii) Se $A \subseteq B$, logo $P(A) \leq P(B)$.

Observe que a Propriedade $[\mathbf{P}_3]$ no Teorema 7.1 fornece a probabilidade da união de eventos no caso em que eles são disjuntos. A fórmula geral (demonstrada no Problema 7.14) é chamada de Princípio da Adição. Especificamente:

Teorema 7.4 (Princípio da Adição): Para quaisquer eventos A e B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Exemplo 7.6 Suponha que um estudante é selecionado aleatoriamente entre 100 alunos, onde 30 estudam matemática, 20 estudam química e 10 estudam matemática e química. Encontre a probabilidade p de que o aluno esteja estudando matemática ou química.

Seja $M = \{\text{alunos estudando matemática}\}$ e $C = \{\text{alunos estudando química}\}$. Como o espaço é equiprovável,

$$P(M) = \frac{30}{100} = \frac{3}{10},\ P(C) = \frac{20}{100} = \frac{1}{5},\ P(M \text{ e } C) = P(M \cap C) = \frac{10}{100} = \frac{1}{10}$$

Assim, pelo Princípio da Adição (Teorema 7.4),

$$p = P(M \text{ ou } C) = P(M \cup C) = P(M) + P(C) - P(M \cap C) = \frac{3}{10} + \frac{1}{5} - \frac{1}{10} = \frac{2}{5}$$

7.4 PROBABILIDADE CONDICIONAL

Suponha que E é um evento em um espaço amostral S com $P(E) > 0$. A probabilidade de que um evento A ocorra, uma vez que E tenha ocorrido, ou, especificamente, a *probabilidade condicional de A dado E*, escrita $P(A|E)$, é definida como se segue:

$$P(A|E) = \frac{P(A \cap E)}{P(E)}$$

Como representado no diagrama de Venn da Fig. 7-3, $P(A|E)$ mede, em certo sentido, a probabilidade relativa de A em relação ao espaço reduzido E.

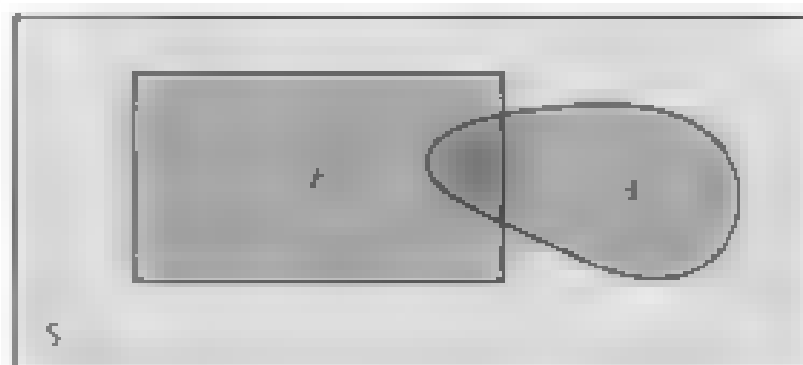



Figura 7-3

Suponha que S é um espaço equiprovável, e $n(A)$ denota o número de elementos de A. Então:

$$P(A \cap E) = \frac{n(A \cap E)}{n(S)}, \quad P(E) = \frac{n(E)}{n(S)}, \quad \text{e, assim,} \quad P(A|E) = \frac{P(A \cap E)}{P(E)} = \frac{n(A \cap E)}{n(E)}$$

Estabelecemos esse resultado formalmente.

Teorema 7.5: Suponha que S é um espaço equiprovável e A e E são eventos. Então

$$P(A|E) = \frac{\text{número de elementos em } A \cap E}{\text{número de elementos em } E} = \frac{n(A \cap E)}{n(E)}$$

Exemplo 7.7

(a) Um par de dados não viciados é jogado. O espaço amostral S consiste dos 36 pares ordenados (a, b), onde a e b podem ser qualquer um dos inteiros de 1 a 6. (Ver Exemplo 7.2.) Assim, a probabilidade de qualquer ponto é $\frac{1}{36}$. Encontre a probabilidade de que um dos dados seja 2 se a soma é 6. Ou seja, determine $P(A|E)$, onde:

$$E = \{\text{soma é } 6\} \text{ e } A = \{2 \text{ aparece em pelo menos um dado}\}$$

Agora E consiste em 5 elementos e $A \cap E$ é formado por 2 elementos, pois

$$E = \{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\} \text{ e } A \cap E = \{(2, 4), (4, 2)\}$$

Pelo Teorema 7.5, $P(A|E) = 2/5$.

Por outro lado, A consiste de 11 elementos, isto é,

$$A = \{(2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (1, 2), (3, 2), (4, 2), (5, 2), (6, 2)\}$$

Como S tem 36 elementos, $P(A) = 11/36$.

(b) Um casal tem dois filhos, o espaço amostral é $S = \{mm, mf, fm, ff\}$ com probabilidade $\frac{1}{4}$ para cada ponto. Encontre a probabilidade p de que ambas as crianças sejam do sexo masculino se for sabido que: (i) pelo menos uma das crianças é do sexo masculino; (ii) a criança mais velha é do sexo masculino.

(i) Aqui o espaço reduzido consiste em três elementos, $\{mm, mf, fm\}$; logo, $p = \frac{1}{3}$.

(ii) Aqui o espaço reduzido consiste em apenas dois elementos $\{mm, mf\}$, logo, $p = \frac{1}{2}$.

Teorema da multiplicação para probabilidade condicional

Suponha que A e B sejam eventos de um espaço amostral S com $P(A) > 0$. Pela definição de probabilidade condicional,

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

Multiplicando ambos os lados por $P(A)$, temos o seguinte resultado útil.

Teorema 7.6 (teorema da multiplicação para probabilidade condicional):

$$P(A \cap B) = P(A)P(B|A)$$

O teorema da multiplicação nos fornece uma fórmula para a probabilidade de que ambos os eventos A e B ocorram. Ela pode ser facilmente estendida para três ou mais eventos, $A_1, A_2, \ldots, A_m$; ou seja,

$$P(A_1 \cap A_2 \cap \cdots A_m) = P(A_1) \cdot P(A_2|A_1) \cdots P(A_m|A_1 \cap A_2 \cap \cdots \cap A_{m-1})$$

Exemplo 7.8 Um lote contém 12 itens, dos quais 4 são defeituosos. Três itens são escolhidos aleatoriamente a partir do lote, um após o outro. Encontre a probabilidade p de que os três sejam não defeituosos.

A probabilidade de que o primeiro item seja não defeituoso é $\frac{8}{12}$, uma vez que 8 entre 12 itens não apresentam defeito. Se o primeiro item é não defeituoso, então a probabilidade de que o próximo esteja sem defeito é de $\frac{7}{11}$, uma vez que 7 dos 11 restantes são não defeituosos. Se os dois primeiros itens não têm defeito, então a probabilidade de que o último não seja defeituoso é de $\frac{6}{10}$, pois apenas 6 dos 10 agora são sem defeito. Logo, pelo teorema da multiplicação,

$$p = \frac{8}{12} \cdot \frac{7}{11} \cdot \frac{6}{10} = \frac{14}{55} \approx 0{,}25$$

7.5 EVENTOS INDEPENDENTES

Eventos A e B em um espaço de probabilidades S são ditos *independentes* se a ocorrência de um deles não influencia a ocorrência do outro. Mais especificamente, B é independente de A se $P(B)$ é igual a $P(B|A)$. Agora, substituindo $P(B|A)$ por $P(B)$ no teorema da multiplicação, $P(A \cap B) = P(A)P(B|A)$ nos leva a

$$P(A \cap B) = P(A)P(B)$$

Usamos formalmente a equação acima como nossa definição de independência.

Definição 7.2: Eventos A e B são *independentes* se $P(A \cap B) = P(A)P(B)$, caso contrário, eles são *dependentes*

Enfatizamos que independência é uma relação simétrica. Em particular, a equação

$$P(A \cap B) = P(A)P(B) \text{ implica que } P(B|A) = P(B) \text{ e } P(A|B) = P(A)$$

Exemplo 7.9 Uma moeda não viciada é jogada três vezes, resultando no espaço equiprovável

$$S = \{AAA, AAO, AOA, AOO, OAA, OAO, OOA, OOO\}$$

Considere os eventos:

$$\begin{aligned} A &= \{\text{primeira jogada é cara}\} = \{AAA, AAO, AOA, AOO\} \\ B &= \{\text{segunda jogada é cara}\} = \{AAA, AAO, OAA, OAO\} \\ C &= \{\text{exatamente duas caras seguidas}\} = \{AAO, OAA\} \end{aligned}$$

Claramente, A e B são eventos independentes, este fato é verificado abaixo. Por outro lado, a relação entre A e C e entre B e C não é óbvia. Afirmamos que A e C são independentes, mas que B e C são dependentes. Temos

$$P(A) = \frac{4}{8} = \frac{1}{2} \qquad P(B) = \frac{4}{8} = \frac{1}{2} \qquad P(C) = \frac{2}{8} = \frac{1}{4}$$

Também,

$$P(A \cap B) = P(\{AAA, AAO\}) = \frac{1}{4},\ P(A \cap C) = P(\{AAO\}) = \frac{1}{8},\ P(B \cap C) = P(\{AAO, OAA\}) = \frac{1}{4}$$

Consequentemente,

$$P(A)P(B) = \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{4} = P(A \cap B) \text{ e, assim, } A \text{ e } B \text{ são independentes}$$
$$P(A)P(C) = \tfrac{1}{2} \cdot \tfrac{1}{4} = \tfrac{1}{8} = P(A \cap C) \text{ e, assim, } A \text{ e } C \text{ são independentes}$$
$$P(B)P(C) = \tfrac{1}{2} \cdot \tfrac{1}{4} = \tfrac{1}{8} \neq P(B \cap C) \text{ e, assim, } B \text{ e } C \text{ são dependentes.}$$

Frequentemente, postulamos que dois eventos são independentes ou o experimento em si implica que dois eventos são independentes.

Exemplo 7.10 A probabilidade de que A atinja um alvo é $\frac{1}{4}$, e a probabilidade de que B atinja o alvo é de $\frac{2}{5}$. Ambos atiram no alvo. Encontre a probabilidade de que pelo menos um deles atinja o alvo, ou seja, que A ou B (ou ambos) acertem no alvo.

Sabemos que $P(A) = \frac{1}{4}$ e $P(B) = \frac{2}{5}$, e procuramos $P(A \cup B)$. Além disso, a probabilidade de que A ou B atinja o alvo não é influenciada pelo que o outro faz, isto é, o evento de que A atinja o alvo é independente do evento de que B acerte no alvo; ou seja, $P(A \cap B) = P(A)P(B)$. Assim,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = P(A) + P(B) - P(A)P(B) = \tfrac{1}{4} + \tfrac{2}{5} - \left(\tfrac{1}{4}\right)\left(\tfrac{2}{5}\right) = \tfrac{11}{20}$$

7.6 TENTATIVAS INDEPENDENTES REPETIDAS, DISTRIBUIÇÃO BINOMIAL

Discutimos anteriormente espaços de probabilidades que são associados com um experimento repetido um número finito de vezes, como a jogada de uma moeda três vezes. Esse conceito de repetição é formalizado como se segue:

Definição 7.3: Seja S um espaço de probabilidades finito. Por espaço de *n tentativas independentes repetidas*, queremos dizer o espaço de probabilidades S_n consistindo em n-uplas ordenadas de elementos de S, com a probabilidade de uma n-upla definida como o produto das probabilidades de suas componentes:

$$P((s_1, s_2, \ldots, s_n)) = P(s_1)\,P(s_2)\ldots P(s_n)$$

Exemplo 7.11 Sempre que três cavalos a, b e c correm juntos, suas respectivas probabilidades de vencer são $\frac{1}{2}$, $\frac{1}{3}$ e $\frac{1}{6}$. Em outras palavras, $S = \{a, b, c\}$ com $P(a) = \frac{1}{2}$, $P(b) = \frac{1}{3}$ e $P(c) = \frac{1}{6}$. Se os cavalos correm duas vezes, então o espaço amostral das duas tentativas repetidas é

$$S_2 = \{aa, ab, ac, ba, bb, bc, ca, cb, cc\}$$

Por conveniência de notação, escrevemos ac para o par ordenado (a, c). A probabilidade de cada ponto em S_2 é

$$P(aa) = P(a)P(a) = \tfrac{1}{2}\left(\tfrac{1}{2}\right) = \tfrac{1}{4} \qquad P(ba) = \tfrac{1}{6}, \qquad P(ca) = \tfrac{1}{12}$$
$$P(ab) = P(a)P(b) = \tfrac{1}{2}\left(\tfrac{1}{3}\right) = \tfrac{1}{6} \qquad P(bb) = \tfrac{1}{9}, \qquad P(cb) = \tfrac{1}{18}$$
$$P(ac) = P(a)P(c) = \tfrac{1}{2}\left(\tfrac{1}{6}\right) = \tfrac{1}{12} \qquad P(bc) = \tfrac{1}{18}, \qquad P(cc) = \tfrac{1}{36}$$

Assim, a probabilidade de c vencer a primeira corrida e a vencer a segunda é $P(ca) = \frac{1}{12}$.

Tentativas repetidas com dois resultados, tentativas de Bernoulli, experimento binomial

Agora considere um experimento com apenas dois resultados. Tentativas independentes repetidas de tal experimento são chamadas de tentativas de Bernoulli, em homenagem ao matemático suíço Jacob Bernoulli (1654-1705). O termo tentativas independentes significa que o resultado de qualquer tentativa não depende dos resultados anteriores (como o jogar de uma moeda). Chamamos um dos resultados de *sucesso* e o outro de *fracasso*.

Seja p a probabilidade de sucesso em uma tentativa de Bernoulli, e assim $q = 1 - p$ é a probabilidade de fracasso. Um *experimento binomial* consiste em um número fixo de tentativas de Bernoulli. Um experimento binomial com n tentativas e probabilidade p de sucesso é denotado por

$$B(n, p)$$

Frequentemente, estamos interessados no número de sucessos em um experimento binomial e não na ordem em que eles ocorrem. O teorema a seguir (demonstrado no Problema 7.27) se aplica. Observamos que o teorema emprega o seguinte coeficiente binomial que é discutido detalhadamente no Capítulo 5.

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)(k-2)\cdots 3\cdot 2\cdot 1} = \frac{n!}{k!(n-k)!}$$

Teorema 7.7: A probabilidade de exatamente k sucessos em um experimento binomial $B(n, p)$ é dada por

$$P(k) = P(k \text{ sucessos}) = \binom{n}{k} p^k q^{n-k}$$

A probabilidade de um ou mais sucessos é $1 - q^n$.

Exemplo 7.12 Uma moeda não viciada é jogada 6 vezes; chamamos o resultado cara de sucesso. Esse é um experimento binomial com $n = 6$ e $p = q = \frac{1}{2}$.

(a) A probabilidade de que exatamente duas caras ocorram (isto é, $k = 2$) é

$$P(2) = \binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4 = \frac{15}{64} \approx 0{,}23$$

(b) A probabilidade de se obter pelo menos quatro caras (ou seja, $k = 4$, 5 ou 6) é

$$\begin{aligned} P(4) + P(5) + P(6) &= \binom{6}{4}\left(\frac{1}{2}\right)^4\left(\frac{1}{2}\right)^2 + \binom{6}{4}\left(\frac{1}{2}\right)^4\left(\frac{1}{2}\right)^2 + \binom{6}{6}\left(\frac{1}{2}\right)^6 \\ &= \frac{15}{64} + \frac{6}{64} + \frac{1}{64} = \frac{11}{32} \approx 0{,}34 \end{aligned}$$

(c) A probabilidade de não conseguir caras (isto é, somente fracassos) é $q^6 = \left(\frac{1}{2}\right)^6 = \frac{1}{64}$. Assim, a probabilidade de uma ou mais caras é $1 - q^n = 1 - \frac{1}{64} = \frac{63}{64} \approx 0{,}94$.

Observação: A função $P(k)$ para $k = 0, 1, 2, \ldots, n$, em um experimento binomial $B(n, p)$ é chamada de *distribuição binomial*, uma vez que ela corresponde aos termos sucessivos da expansão binomial

$$(q + p)^n = q^n + \binom{n}{1}q^{n-1}p + \binom{n}{2}q^{n-2}p^2 + \cdots + p^n$$

O uso do termo *distribuição* é explicado adiante no capítulo.

7.7 VARIÁVEIS ALEATÓRIAS

Seja S uma amostra de um experimento. Como anteriormente observado, o resultado do experimento, ou os pontos de S, não precisam ser números. Por exemplo, jogando uma moeda, os resultados são A (cara) ou O (coroa); e jo-

gando um par de dados, os resultados são pares de inteiros. No entanto, frequentemente desejamos assinalar um número específico para cada resultado do experimento. Por exemplo, no jogo de cara ou coroa, pode ser conveniente assinalar 1 para A e 0 para O; ou, no jogo de um par de dados, podemos querer assinalar a soma dos dois inteiros ao resultado. Tal correspondência de valores numéricos é chamada de *variável aleatória*. Generalizando, temos a seguinte definição.

Definição 7.4: Uma *variável aleatória* X é uma regra que designa um valor numérico para cada resultado de um espaço amostral S.

Denotamos por R_X o conjunto de números designados por uma variável aleatória X, e nos referimos a R_X como o *espaço imagem*.

Observação: Em terminologia mais formal, X é uma função de S nos números reais $\mathbf{R}$, e R_X é a imagem de X. Além disso, para alguns espaços amostrais infinitos S, nem todas as funções de S em $\mathbf{R}$ são consideradas variáveis aleatórias. Contudo, os espaços amostrais aqui são finitos, e toda função real definida sobre um espaço amostral finito é uma variável aleatória.

Exemplo 7.13 Um par de dados não viciados é jogado. (Ver Exemplo 7.2.) O espaço amostral S consiste nos 36 pares ordenados (a, b), onde a e b podem ser qualquer um dos inteiros de 1 a 6.
Faça X assinalar a cada ponto de S a soma dos números, então X é uma variável aleatória com espaço imagem

$$R_X = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

Faça Y assinalar a cada ponto o maior dos dois números; então Y é uma variável aleatória com espaço imagem

$$R_Y = \{1, 2, 3, 4, 5, 6\}$$

Somas e produtos de variáveis aleatórias, notação

Suponha que X e Y sejam variáveis aleatórias sobre o mesmo espaço amostral S. Então $X + Y$, kX e XY são funções sobre S e definidas como se segue (onde $s \in S$):

$$(X + Y)(s) = X(s) + Y(s), \; (kX)(s) = kX(s), \; (XY)(s) = X(s)Y(s)$$

Genericamente, para qualquer função polinomial ou exponencial $h(x, y, \ldots, z)$, definimos $h(X, Y, \ldots, Z)$ como sendo a função sobre S definida por

$$[h(X, Y, \ldots, Z)](s) = h[X(s), Y(s), \ldots, Z(s)]$$

É possível mostrar que essas também são variáveis aleatórias. (Isso é trivial no caso em que todo subconjunto de S é um evento.)

As notações abreviadas $P(X = a)$ e $P(a \leq X \leq b)$ são usadas, respectivamente, para as probabilidades de que "X mapeia em a" e "X mapeia no intervalo $[a, b]$". Ou seja, para $s \in S$:

$$P(X = a) = P(\{s \mid X(s) = a\}) \text{ e } P(a < X < b) = P(\{s \mid a < X(s) < b\})$$

Significados análogos são dados para $P(X \leq a)$, $P(X = a, Y = b)$, $P(a \leq X \leq b, c \leq Y \leq d)$, e assim por diante.

Distribuição de probabilidade de uma variável aleatória

Seja X uma variável aleatória sobre um espaço amostral finito S com espaço imagem $R_x = \{x_1, x_2, \ldots, x_t\}$. Então X induz uma função f que assinala probabilidades p_k aos pontos x_k de R_x como se segue:

$$f(x_k) = p_k = P(X = x_k) = \text{soma de probabilidades de pontos de } S \text{ cuja imagem é } x_k.$$

O conjunto de pares ordenados $(x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_t, f(x_t))$ é conhecido como a *distribuição* da variável aleatória X; ela geralmente é dada por uma tabela como na Fig. 7-4. Essa função f tem as duas propriedades a seguir:

$$\text{(i) } f(x_k) \geq 0 \quad \text{e} \quad \text{(ii) } \sum_k f(x_k) = 1$$

Assim R_X com a correspondência acima de probabilidades é um espaço de probabilidades. (Às vezes usamos a notação $[x_k, p_k]$ para denotar a distribuição de X no lugar de $[x, f(x)]$).

Resultado x	x_1	x_2	x_3	…	x_t
Probabilidade $f(x)$	$f(x_1)$	$f(x_2)$	$f(x_3)$	…	$f(x_t)$

Figura 7-4 Distribuição f de uma variável aleatória X.

No caso em que S é um espaço equiprovável, podemos facilmente obter a distribuição de uma variável aleatória a partir do seguinte resultado.

Teorema 7.8: Sejam S um espaço equiprovável e f a distribuição de uma variável aleatória X sobre S com o espaço imagem $R_X = \{x_1, x_2, \ldots, x_t\}$. Então

$$p_i = f(x_i) = \frac{\text{número de pontos de } S \text{ cujas imagens são } x_i}{\text{número de pontos em } S}$$

Exemplo 7.14 Seja X a variável aleatória do Exemplo 7.13 que assinala a soma do jogo de um par de dados. Observe que $n(S) = 36$ e $R_x = \{2, 3, \ldots, 12\}$. Usando o Teorema 7.8, obtemos a distribuição f de X como se segue:

$f(2) = 1/36$, pois há um resultado (1, 1) cuja soma é 2.
$f(3) = 2/36$, pois há dois resultados (1, 2) e (2, 1) cuja soma é 3.
$f(4) = 3/36$, pois há três resultados (1, 3), (2, 2) e (3, 1) cuja soma é 4.

Analogamente, $f(5) = 4/36, f(6) = 5/36, \ldots, f(12) = 1/36$. Assim, a distribuição de X é a que segue.

x	2	3	4	5	6	7	8	9	10	11	12
$f(x)$	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36

Valor esperado de uma variável aleatória

Seja X uma variável aleatória sobre um espaço de probabilidades $S = \{s_1, s_2, \ldots, s_m\}$. Então a *média* ou *valor esperado* de X é denotado e definido por:

$$\mu = E(X) = X(s_1)P(s_1) + X(s_2)P(sa_2) + \cdots + X(s_m)P(s_m) = \sum X(s_k)P(s_k)$$

Especificamente, se X é dada pela distribuição f da Fig. 7-4, então o valor esperado de X é:

$$\mu = E(X) = x_1 f(x_1) + x_2 f(x_2) + \cdots + x_t f(x_t) = \sum x_k f(x_k)$$

Alternativamente, quando a notação $[x_k, p_k]$ é empregada no lugar de $[x_k, f(x_k)]$,

$$\mu = E(X) = x_1 p_1 + x_2 p_2 + \cdots + x_t p_t = \sum x_i p_i$$

(Por conveniência notacional, omitimos os índices no símbolo somatório Σ.)

Exemplo 7.15

(a) Suponha que uma moeda não viciada é jogada seis vezes. O número de caras que podem ocorrer com suas respectivas probabilidades segue:

x_i	0	1	2	3	4	5	6
p_i	1/64	6/64	15/64	20/64	15/64	6/64	1/64

Então a média ou valor esperado (ou número esperado de caras) é:

$$\mu = E(X) = 0\left(\tfrac{1}{64}\right) + 1\left(\tfrac{6}{64}\right) + 2\left(\tfrac{15}{64}\right) + 3\left(\tfrac{20}{64}\right) + 4\left(\tfrac{15}{64}\right) + 5\left(\tfrac{6}{64}\right) + 6\left(\tfrac{1}{64}\right) = 3$$

(Isso está de acordo com nossa intuição de que metade das jogadas são caras.)

(b) Três cavalos a, b e c estão em uma corrida, suponha que suas respectivas probabilidades de vencer sejam $\frac{1}{2}$, $\frac{1}{3}$ e $\frac{1}{6}$. Seja X a função de pagamento para o cavalo vencedor, e suponha que X paga \$2, \$6 e \$9 se a, b ou c ganhar a corrida. O pagamento esperado para a corrida é

$$\begin{aligned} E(X) &= X(a)P(a) + X(b)P(b) + X(c)P(c) \\ &= 2\left(\tfrac{1}{2}\right) + 6\left(\tfrac{1}{3}\right) + 9\left(\tfrac{1}{6}\right) = 4{,}5 \end{aligned}$$

Variância e desvio padrão de uma variável aleatória

Seja X uma variável aleatória com média μ e distribuição f, como na Fig. 7-4. Então a variância de X, denotada por $Var(X)$, é definida como:

$$Var(X) = (x_1 - \mu)^2 f(x_1) + (x_2 - \mu)^2 f(x_2) + \cdots + (x_t - \mu)^2 f(x_t) = \Sigma(x_k - \mu)^2 f(x_k) = E((X - \mu)^2)$$

Alternativamente, quando a notação $[x_k, p_k]$ é empregada no lugar de $[x_k, f(x_k)]$,

$$Var(X) = (x_1 - \mu)^2 p_1 + (x_2 - \mu)^2 p_2 + \cdots + (x_t - \mu)^2 p_t = \Sigma(x_k - \mu)^2 p_k = E((X - \mu)^2)$$

O *desvio padrão* de X, denotado por σ_X, ou simplesmente σ, é a raiz quadrada não negativa de $Var(X)$:

$$\sigma_X = \sqrt{Var(X)}$$

Consequentemente, $Var(X) = \sigma_X{}^2$. Ambos $Var(X)$ e $\sigma_X{}^2$, ou simplesmente σ^2, são utilizados para denotar a variância de X.

As fórmulas a seguir são comumente mais convenientes para calcular $Var(X)$ do que apresentamos acima

$$Var(X) = x_1{}^2 f(x_1) + x_2{}^2 f(x_2) + \cdots + x_t{}^2 f(x_t) - \mu^2 = \left[\sum x_k{}^2 f(x_k)\right] - \mu^2 = E(X^2) - \mu^2$$

ou

$$Var(X) = x_1{}^2 p_1 + x_2{}^2 p_2 + \cdots + x_t{}^2 p_t - \mu^2 = \left[\sum x_k^2 p_k\right] - \mu^2 = E(X^2) - \mu^2$$

Exemplo 7.16 Seja X o número de vezes que ocorre cara quando uma moeda não viciada é jogada seis vezes. A distribuição de X aparece no Exemplo 7.15(a), onde sua média $\mu = 3$ é calculada. A variância de X é computada como se segue:

$$Var(X) = (0 - 3)^2 \tfrac{1}{64} + (1 - 3)^2 \tfrac{6}{64} + (2 - 3)^2 \tfrac{15}{64} + \cdots + (6 - 3)^2 \tfrac{1}{64} = 1{,}5$$

Alternativamente,

$$Var(X) = 0^2\tfrac{1}{64} + 1^2\tfrac{6}{64} + 2^2\tfrac{15}{64} + 3^2\tfrac{20}{64} + 4^2\tfrac{15}{64} + 5^2\tfrac{6}{64} + 6^2\tfrac{1}{64} - 3^2 = 1,5$$

Assim, o desvio padrão é $\sigma = \sqrt{1,5} \approx 1,225$ (caras).

Distribuição binomial

Considere um experimento binomial $B(n, p)$. Ou seja, $B(n, p)$ consiste em n tentativas independentes repetidas com dois resultados, sucesso ou fracasso, e p é a probabilidade de sucesso (e $q = (1 - p)$ é a probabilidade de fracasso). O número X de k sucessos é uma variável aleatória com distribuição aparecendo na Fig. 7-5.

Número de sucessos k	0	1	2	...	n
Probabilidade $P(k)$	q^n	$\binom{n}{1} q^{n-1}p$	$\binom{n}{2} q^{n-2}p^2$	...	p^n

Figura 7-5

O teorema a seguir se aplica.

Teorema 7.9: Considere a distribuição binomial $B(n, p)$. Então:

(i) Valor esperado $E(X) = \mu = np$.

(ii) Variância $Var(X) = \sigma^2 = npq$.

(iii) Desvio padrão $\sigma = \sqrt{npq}$.

Exemplo 7.17

(a) A probabilidade de que um homem acerte em um alvo é $p = 1/5$. Ele dispara 100 vezes. Encontre o número esperado μ de vezes que ele atinja o alvo e o desvio padrão σ.

Aqui $p = \frac{1}{5}$ e, portanto, $q = \frac{4}{5}$. Logo,

$$\mu = np = 100 \cdot \frac{1}{5} = 20 \quad \text{e} \quad \sigma = \sqrt{npq} = \sqrt{100 \cdot \frac{1}{5} \cdot \frac{4}{5}} = 4$$

(b) Encontre o número esperado $E(X)$ de respostas corretas conseguidas por acaso em uma avaliação de cinco questões do tipo falso-verdadeiro. Aqui $p = \frac{1}{2}$. Logo, $E(X) = np = 5 \cdot \frac{1}{2} = 2,5$.

7.8 DESIGUALDADE DE CHEBYSHEV, LEI DOS GRANDES NÚMEROS

O desvio padrão σ de uma variável aleatória x mede o espalhamento ponderado dos valores de X em torno da média μ. Assim, para um σ menor, esperamos que X fique mais próximo de μ. Uma afirmação mais precisa dessa expectativa é dada pela seguinte desigualdade, que homenageia o matemático russo P. L. Chebyshev (1821-1894).

Teorema 7.10 (Desigualdade de Chebyshev). Seja X uma variável aleatória com média μ e desvio padrão σ. Então, para qualquer número positivo k, a probabilidade de que um valor de X esteja no intervalo $[\mu - k\sigma, \mu + k\sigma]$ é de pelo menos $1 - 1/k^2$. Ou seja,

$$P(\mu - k\sigma \le X \le \mu + k\sigma) \ge 1 - \frac{1}{k^2}$$

Exemplo 7.18 Suponha que X é uma variável aleatória com média $\mu = 75$ e desvio padrão $\sigma = 5$. Qual conclusão sobre X pode ser derivada da Desigualdade de Chebyshev para $k = 2$ e $k = 3$?

Fazendo $k = 2$, obtemos

$$\mu - k\sigma = 75 - 2(5) = 65 \text{ e } \mu + k\sigma = 75 + 2(5) = 85$$

Logo, podemos concluir que a probabilidade de que um valor de X esteja entre 65 e 85 é de pelo menos $1 - (1/2)^2 = 3/4$; ou seja,

$$P(65 \leq X \leq 85) \geq 3/4$$

Analogamente, fazendo $k = 3$, podemos concluir que a probabilidade de que um valor de X esteja entre 60 e 90 é de pelo menos $1 - (1/3)^2 = 8/9$.

Média da amostra e Lei dos Grandes Números

Considere um número finito de variáveis aleatórias $X, Y, \ldots, Z$ em um espaço amostral S. Elas são ditas *independentes* se, para quaisquer valores $x_i, y_j, \ldots, z_k$,

$$P(X = x_i, Y = y_j, \ldots, Z = z_k) = P(X = x_i)\,P(Y = y_j) \ldots P(Z = z_k)$$

Especificamente, X e Y são independentes se

$$P(X = x_i, Y = y_j) = P(X = x_i)\,P(Y = y_j)$$

Agora seja X uma variável aleatória com média μ. Podemos considerar o resultado numérico de cada uma das n tentativas independentes como uma variável aleatória com a mesma distribuição de X. A variável aleatória correspondente ao i-ésimo resultado é denotada por X_i ($i = 1, 2, \ldots, n$). (Observamos que os X_i são independentes com a mesma distribuição de X.) O valor médio de todos os n resultados é também uma variável aleatória, denotada por $\bar{X}_n$ e chamada de *média da amostra*. Ou seja:

$$\bar{X}_n = \frac{X_1 + X_2 + \cdots + X_n}{n}$$

A Lei dos grandes números diz que, à medida que n aumenta de valor, a média da amostra $\bar{X}_n$ se aproxima do valor médio μ. Ou seja:

Teorema 7.11 (Lei dos Grandes Números): Para qualquer número positivo α, não importando o quão pequeno seja, a probabilidade de que a média da amostra $\bar{X}_n$ tenha um valor no intervalo $[\mu - \alpha, \mu + \alpha]$ se aproxima de 1 quando n tende ao infinito. Isto é:

$$P([\mu - \alpha \leq \bar{X} \leq \mu + \alpha]) \to 1 \text{ quando } n \to \infty$$

Exemplo 7.19 Suponha que um dado seja jogado 5 vezes com resultados

$$x_1 = 3, x_2 = 4, x_3 = 6, x_4 = 1, x_5 = 4$$

Então o correspondente valor $\bar{x}$ da média da amostra $\bar{X}_5$ é o que se segue:

$$\bar{x} = \frac{3 + 4 + 6 + 1 + 4}{5} = 3{,}6$$

Para um dado justo, a média $\mu = 3{,}5$. A Lei dos Grandes Números nos diz que, quando n se torna maior, existe uma probabilidade maior de que $\bar{X}_n$ se aproxime de 3,5.

Problemas Resolvidos

7.1 Considere uma moeda e um dado sendo jogados, e seja S o espaço amostral consistindo nos 12 elementos:

$$S = \{A1, A2, A3, A4, A5, A6, O1, O2, O3, O4, O5, O6\}$$

(*a*) Escreva explicitamente os seguintes eventos:

$$A = \{\text{caras e um número par}\},\ B = \{\text{número primo}\},\ C = \{\text{coroas e um número ímpar}\}$$

(*b*) Escreva explicitamente os eventos: (i) A ou B ocorrem, (ii) B e C ocorrem, (iii) apenas B ocorre.

(*c*) Qual par dos eventos A, B e C são mutuamente exclusivos?

(*a*) Os elementos de A são aqueles de S consistindo em um A e um número par:

$$A = \{A2, A4, A6\}$$

Os elementos de B são aqueles pontos de S cujas segundas componentes são números primos (2, 3 ou 5).

$$B = \{A2, A3, A5, O2, O3, O5\}$$

Os elementos de C são aqueles pontos de S consistindo em um O e um número ímpar: $C = \{O1, O3, O5\}$

(*b*) (i) $A \cup B = \{A2, A4, A6, A3, A5, O2, O3, O5\}$

(ii) $B \cap C = \{O3, O5\}$

(iii) $B \cap A^c \cap C^c = \{A3, A5, O2\}$

(*c*) A e C são mutuamente exclusivos, pois $A \cap C = \varnothing$

7.2 Um par de dados é jogado. (Ver Exemplo 7.2) Encontre o número de elementos em cada evento.

(*a*) $A = \{\text{dois números são iguais}\}$ (*c*) $C = \{\text{5 aparece no primeiro dado}\}$

(*b*) $B = \{\text{a soma é 10 ou mais}\}$ (*d*) $D = \{\text{5 aparece em pelo menos um dado}\}$

Use a Fig. 7-1(*b*) para ajudar a contar o número de elementos no evento.

(*a*) $A = \{(1, 1), (2, 2), \ldots, (6, 6)\}$, assim $n(A) = 6$.

(*b*) $B = \{(6, 4), (5, 5), (4, 6), (6, 5), (5, 6), (6, 6)\}$, logo $n(B) = 6$.

(*c*) $C = \{(5, 1), (5, 2), \ldots, (5, 6)\}$, portanto $n(C) = 6$.

(*d*) Há seis pares com 5 como primeiro elemento, e seis pares com 5 como segundo elemento. Contudo, (5, 5) aparece em ambos os lugares. Logo,

$$n(D) = 6 + 6 - 1 = 11$$

Alternativamente, conte os pares na Fig. 7-1(*b*) que estão em D, para obter $n(D) = 11$.

Espaços equiprováveis finitos

7.3 Determine a probabilidade p de cada evento:

(*a*) Um número par aparece na jogada de um dado justo;

(*b*) Uma ou mais caras aparecem na jogada de três moedas justas;

(*c*) Uma pedra vermelha aparece em uma retirada aleatória de uma caixa contendo quatro pedras brancas, três vermelhas e cinco azuis.

Cada espaço amostral S é equiprovável. Assim, para cada evento E usamos

$$P(E) = \frac{\text{número de elementos em } E}{\text{número de elementos em } S} = \frac{n(E)}{n(S)}$$

(*a*) O evento pode ocorrer de três maneiras (2, 4 ou 6) em um total de seis casos, logo, $p = \frac{3}{6} = \frac{1}{2}$.

(*b*) Há oito casos:

$$AAA, AAO, AOA, AOO, OAA, OAO, OOA, OOO$$

Apenas o último caso não é favorável, logo, $p = 7/8$.

(*c*) Há $4 + 3 + 5 = 12$ pedras, das quais três são vermelhas; portanto, $p =$ [illegible].

7.4 Uma única carta é retirada de um baralho comum com 52 cartas. (Ver Fig. 7-2.) Encontre a probabilidade p de que a carta seja.

(*a*) pictórica (valete, dama ou rei); (*c*) pictórica e de copas,

(*b*) de copas; (*d*) pictórica ou de copas.

Aqui $n(S) = 52$.

(*a*) Há $4(3) = 12$ cartas pictóricas; logo, $p = \frac{12}{52} = \frac{3}{13}$

(*b*) Há 13 cartas de copas; logo, $p = \frac{13}{52} = \frac{1}{4}$

(*c*) Há três cartas pictóricas que são de copas; logo, $p = \frac{3}{52}$

(*d*) Fazendo $F = \{\text{cartas pictóricas}\}$ e $H = \{\text{cartas de copas}\}$, temos

$$n(F \cup H) = n(F) + n(H) - n(F \cap H) = 12 + 13 - 3 = 22$$

Portanto, $p = \frac{22}{52} =$ [illegible]

7.5 Duas cartas são retiradas aleatoriamente de um baralho comum de 52 cartas. Encontre a probabilidade p de que: (*a*) ambas sejam de espadas; (*b*) uma seja de espadas e outra de copas.

Existem $\binom{52}{2} = 1326$ maneiras de retirar duas entre 52 cartas.

(*a*) Há $\binom{13}{2} = 78$ maneiras de retirar duas cartas de espadas entre 13; logo,

$$p = \frac{\text{número de maneiras que duas cartas de espadas podem ser retiradas}}{\text{número de maneiras que duas cartas podem ser retiradas}} = \frac{78}{1326} = \frac{3}{5\ldots}$$

(*b*) Existem 13 cartas de espadas e 13 de copas; logo, há $13 \cdot 13 = 169$ maneiras de retirar uma carta de espadas e uma de copas. Assim, p [illegible]

7.6 Considere o espaço amostral do Problema 7.1. Assuma que a moeda e o dado não são viciados, assim S é um espaço equiprovável. Encontre.

(*a*) $P(A), P(B), P(C)$

(*b*) $P(A \cup B), P(B \cap C), P(B \cap A^C \cap C^C)$

Como S é um espaço equiprovável, use $P(E) = n(E)/n(S)$. Aqui $n(S) = 12$. Portanto, precisamos contar apenas o número de elementos no dado conjunto.

(*a*) $P(A) = \frac{3}{12}$, $P(B) = \frac{6}{12}$, $P(C)$ [illegible]

(*b*) $P(A \cup B) = \frac{8}{12}$, $P(B \cap C) = \frac{2}{12}$, $P(B \cap A^C \cap C^C)$ [illegible]

7.7 Uma caixa contém duas meias brancas e duas azuis. Um par de meias é retirado aleatoriamente. Determine a probabilidade p de que elas casem (têm a mesma cor).

Existem $\binom{4}{2} = 6$ maneiras para retirar duas das meias. Apenas dois pares têm a mesma cor. Logo, $p =$ [illegible]

7.8 Cinco cavalos estão em uma corrida. André escolhe dois dos cavalos aleatoriamente e aposta neles. Encontre a probabilidade p de que André tenha escolhido o vencedor.

Há $\binom{5}{2} = 10$ maneiras de escolher dois dos cavalos. Quatro dos pares terão o vencedor. Assim, $p =$ [illegible]

Espaços finitos de probabilidades

7.9 Um espaço amostral S consiste em quatro elementos, ou seja, $S = \{a_1, a_2, a_3, a_4\}$. Sob a ação de quais das seguintes funções S se torna um espaço de probabilidades?

(*a*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{3}$ $P(a_3) = \frac{1}{4}$ $P(a_4) = \frac{1}{5}$
(*b*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = -\frac{1}{4}$ $P(a_4) = \frac{1}{2}$
(*c*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = \frac{1}{8}$ $P(a_4) = \frac{1}{8}$
(*d*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = \frac{1}{4}$ $P(a_4) = 0$

(*a*) Como a soma dos valores nos pontos amostrais é maior do que um, a função não define S como um espaço de probabilidades.

(*b*) Uma vez que $P(a_3)$ é negativo, a função não define S como um espaço de probabilidades.

(*c*) Como cada valor é não negativo e a soma dos valores é um, a função define S como um espaço de probabilidades.

(*d*) Os valores são não negativos e somam um, logo, a função define S como um espaço de probabilidades

7.10 Uma moeda é viciada de forma que cara é duas vezes mais provável de ocorrer do que coroa. Encontre $P(A)$ e $P(O)$

Seja $P(O) = p$, então $P(A) = 2p$. Agora faça a soma das probabilidades igual a um, isto é, faça $p + 2p = 1$ Então $p = \frac{1}{3}$ Logo, $P(A) = \frac{2}{3}$ e $P(O) = \frac{1}{3}$.

7.11 Suponha que A e B são eventos com $P(A) = 0{,}6$, $P(B) = 0{,}3$ e $P(A \cap B) = 0{,}2$. Encontre a probabilidade de que:

(*a*) A não ocorra; (*c*) A ou B ocorra,

(*b*) B não ocorra; (*d*) Nem A nem B ocorra.

(*a*) P (não A) $= P(A^C) = 1 - P(A) = 0{,}4$.

(*b*) P (não B) $= P(B^C) = 1 - P(B) = 0{,}7$.

(*c*) Pelo Princípio de Adição,

$$\begin{aligned} P\,(A \text{ ou } B) &= P\,(A \cup B) = P\,(A) + P\,(B) - P\,(A \cap B) \\ &= 0{,}6 + 0{,}3 - 0{,}2 = 0{,}7 \end{aligned}$$

(*d*) Lembre que (Lei de DeMorgan) nem A, nem B é o complemento de $A \cup B$ Assim.

$$P\,(\text{nem } A, \text{ nem } B) = P\,((A \cup B)^C) = 1 - P\,(A \cup B) = 1 - 0{,}7 = 0{,}3$$

7.12 Prove o Teorema 7.2: $P(A^c) = 1 - P(A)$

$S = A \cup A^c$, onde A e A^c são disjuntos. Nosso resultado é consequência do seguinte:

$$1 = P(S) = P(A \cup A^c) = P(A) + P(A^c)$$

7.13 Demonstre o Teorema 7.3 (i) $P(\varnothing) = 0$; (ii) $P(A \backslash B) = P(A) - P(A \cap B)$; (iii) Se $A \subseteq B$, então $P(A) \le P(B)$.

(i) $\varnothing = S^c$ e $P(S) = 1$ Logo, $P(\varnothing) = 1 - 1 = 0$.

(ii) Como indicado na Fig 7-6(*a*), $A = (A \backslash B) \cup (A \cap B)$, onde $A \backslash B$ e $A \cap B$ são disjuntos. Portanto,

$$P(A) = P(A \backslash B) + P(A \cap B)$$

A partir disso segue nosso resultado.

(iii) Se $A \subseteq B$, então, como indicado pela Fig 7-6(*b*), $B = A \cup (B \backslash A)$, onde A e $B \backslash A$ são disjuntos. Portanto,

$$P(B) = P(A) + P(B \backslash A)$$

Como $P(B \backslash A) \ge 0$, temos $P(A) \le P(B)$.

(a) A é sombreado

(b) B é sombreado

(c) $A \cup B$ é sombreado

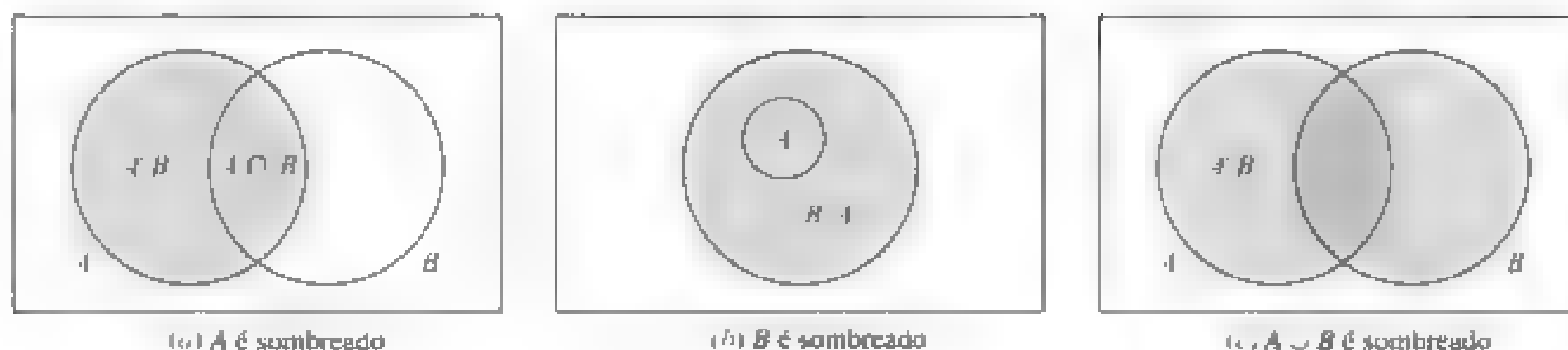



Figura 7-6

7.14 Prove o Teorema 7.4 (Princípio da Adição): Para quaisquer eventos A e B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Como indicado na Fig. 7-6(c), $(A \cup B) = (A \backslash B) \cup B$, onde $A \backslash B$ e B são conjuntos disjuntos. Assim, usando o Teorema 7.3(ii),

$$\begin{aligned} P(A \cup B) &= P(A \backslash B) + P(B) = P(A) - P(A \cap B) + P(B) \\ &= P(A) + P(B) - P(A \cap B) \end{aligned}$$

Probabilidade condicional

7.15 Um par de dados justos é jogado. (Ver Fig. 7-1(b).) Encontre a probabilidade de que a soma seja 10 ou mais se:

(a) 5 ocorre no primeiro dado; (b) 5 ocorre em pelo menos um dado.

(a) Se um 5 ocorre no primeiro dado, então o espaço amostral reduzido é

$$A = \{(5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6)\}$$

A soma é 10 ou maior em dois dos seis resultados: (5, 5), (5, 6). Logo, $p = \frac{2}{6}$

(b) Se um 5 ocorre em pelo menos um dos dados, então o espaço amostral reduzido tem onze elementos

$$B = \{(5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6), (1, 5), (2, 5), (3, 5), (4, 5), (6, 5)\}$$

A soma é maior ou igual a 10 em três dos onze resultados (5, 5), (5, 6), (6, 5). Logo, $p = \frac{3}{11}$

7.16 Em uma certa cidade universitária, 25% dos estudantes reprovaram em matemática (M), 15% reprovaram em ciências (C) e 10% foram reprovados em matemática e ciências. Um estudante é selecionado aleatoriamente.

(a) Se ele reprovou em ciências, encontre a probabilidade de que tenha também reprovado em matemática.

(b) Se ele reprovou em matemática, encontre a probabilidade de que tenha sido reprovado também em ciências.

(c) Encontre a probabilidade de que ele tenha sido reprovado em matemática ou ciências.

(d) Encontre a probabilidade de que ele não tenha sido reprovado nem em matemática nem em ciências.

(a) A probabilidade de que um estudante tenha sido reprovado em matemática, dada a reprovação em ciências, é

$$P(M|C) = \frac{P(M \cap C)}{P(C)} = \frac{0,10}{0,15} = \frac{2}{3}$$

(b) A probabilidade de que um estudante tenha sido reprovado em ciências, dada a reprovação em matemática, é

$$P(C|M) = \frac{P(C \cap M)}{P(M)} = \frac{0,10}{0,25} = \frac{2}{5}$$

(*c*) Pelo Princípio da Adição (Teorema 7.4),

$$P(M \cup C) = P(M) + P(C) - P(M \cap C) = 0{,}25 + 0{,}15 - 0{,}10 = 0{,}30$$

(*d*) Estudantes que não reprovaram nem em matemática nem em ciências formam o complementar do conjunto $M \cup C$, ou seja, eles constituem o conjunto $(M \cup C)^C$. Logo,

$$P((M \cup C)^C) = 1 - P(M \cup C) = 1 - 0{,}30 = 0{,}70$$

7.17 Um par de dados justos é jogado. Dado que dois números que ocorrem são diferentes, encontre a probabilidade p de que. (*a*) a soma seja 6; (*b*) ocorra um 1; (*c*) a soma seja menor ou igual a 4.

Existem 36 maneiras do par de dados ser jogado, e seis delas, (1, 1), (2, 2), . . . , (6, 6), têm os mesmos números. Assim, o espaço amostral reduzido consiste de $36 - 6 = 30$ elementos.

(*a*) A soma 6 pode aparecer de quatro maneiras. (1, 5), (2, 4), (4, 2), (5, 1) (Não podemos incluir (3, 3), uma vez que os números são os mesmos.) Logo, $p =$ [illegible] $=$ [illegible]

(*b*) Um 1 pode ocorrer de 10 maneiras. (1, 2), (1, 3), . . . , (1, 6) e (2, 1), (3, 1), . . . , (6, 1). Portanto, $p =$ [illegible] $=$ [illegible]

(*c*) A soma menor ou igual a 4 pode ocorrer de quatro maneiras. (3, 1), (1, 3), (2, 1) e (1, 2). Assim, $p =$ [illegible] $=$ [illegible]

7.18 Uma turma tem 12 rapazes e 4 garotas. Suponha que três estudantes são selecionados aleatoriamente a partir da turma. Encontre a probabilidade p de que eles sejam todos rapazes.

A probabilidade de que o primeiro estudante escolhido seja um rapaz é 12/16, pois há 12 rapazes entre 16 estudantes. Se o primeiro é um rapaz, a probabilidade de que o segundo estudante seja um rapaz é de 11/15, uma vez que existem 11 rapazes restantes entre os 15 estudantes. Finalmente, se os dois primeiros são rapazes, então a probabilidade de que o terceiro estudante seja um rapaz é de 10/14, pois restaram 10 rapazes entre os 14 estudantes. Assim, pelo teorema da multiplicação, a probabilidade de que todos os três sejam rapazes é

$$p = \frac{12}{16} \cdot \frac{11}{15} \cdot \frac{10}{14} = \frac{11}{28}$$

Outro método

Há $C(16, 3) = 560$ maneiras de selecionar três estudantes entre os 16, e $C(12, 3) = 220$ maneiras de escolher três rapazes entre 12; logo,

$$p = \frac{220}{560} = \frac{11}{28}$$

Outro Método

Se os estudantes são escolhidos um após o outro, então há $16 \cdot 15 \cdot 14$ maneiras de selecionar três estudantes, e $12 \cdot 11 \cdot 10$ maneiras de escolher três rapazes; logo,

$$p = \frac{12 \cdot 11 \cdot 10}{16 \cdot 15 \cdot 14} = \frac{11}{28}$$

Independência

7.19 A probabilidade de que A atinja um alvo é [illegible], e a probabilidade de que B atinja o alvo é de [illegible]. Ambos atiram no alvo. Encontre a probabilidade de que:

(*a*) A não acerte o alvo; (*c*) um deles atinja o alvo;

(*b*) ambos atinjam o alvo; (*d*) nenhum deles acerte o alvo.

Sabemos que $P(A) =$ [illegible] e $P(B) =$ [illegible] (e assumimos que os eventos são independentes).

(*a*) $P(\text{não } A) = P(A^C) = 1 - P(A) = 1$ [illegible] $=$ [illegible]

(*b*) Como os eventos são independentes,

$$P(A \text{ e } B) = P(A \cap B) = P(A) \cdot P(B) = \text{[illegible]}$$

(*c*) Pelo Princípio da Adição (Teorema 7.4),

$$P(A \text{ ou } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B) = [illegible]$$

(*d*) Temos

$$P(\text{nem } A, \text{ nem } B) = P((A \cup B)^C) = 1 - P(A \cup B) = 1 - [illegible]$$

7.20 Considere os seguintes eventos para uma família com filhos:

$$A = \{\text{filhos de ambos os sexos}\}, \; B = \{\text{no máximo um menino}\}.$$

(*a*) Mostre que A e B são eventos independentes se uma família tem três crianças.

(*b*) Mostre que A e B são eventos dependentes se uma família tem duas crianças.

(*a*) Temos o espaço equiprovável $S = \{mmm, mmf, mfm, mff, fmm, fmg, ffm, fff\}$. Aqui

$$\begin{aligned} A &= \{mmf, mfm, mff, fmm, fmf, ffm\} && \text{e, assim, } P(A) = \tfrac{6}{8} = \tfrac{3}{4} \\ B &= \{mff, fmf, ffm, fff\} && \text{e, assim, } P(B) = \tfrac{4}{8} = [illegible] \\ A \cap B &= \{mff, fmf, ffm\} && \text{e, assim, } P(A \cap B) = [illegible] \end{aligned}$$

Como $P(A)P(B) = \frac{3}{4} \cdot \frac{1}{2} = \frac{3}{8} = P(A \cap B)$, A e B são independentes.

(*b*) Temos o espaço equiprovável $S = \{mm, mf, fm, ff\}$. Aqui

$$\begin{aligned} A &= \{mf, fm\} && \text{e, assim, } P(A) = [illegible] \\ B &= \{mf, fm, ff\} && \text{e, assim, } P(B) = [illegible] \\ A \cap B &= \{mf, fm\} && \text{e, assim, } P(A \cap B) = \tfrac{1}{2} \end{aligned}$$

Como $P(A)P(B) \neq P(A \cap B)$, A e B são dependentes.

7.21 A caixa A contém cinco pedras vermelhas e três azuis, e a caixa B contém três pedras vermelhas e duas azuis. Uma pedra é retirada aleatoriamente de cada caixa.

(*a*) Encontre a probabilidade p de que ambas sejam vermelhas.

(*b*) Encontre a probabilidade p de que uma seja vermelha e outra seja azul.

(*a*) A probabilidade de escolher uma pedra vermelha de A é [illegible] e de B é [illegible]. Como os eventos são independentes, $p =$ [illegible]

(*b*) A probabilidade p_1 de escolher uma pedra vermelha de A e uma azul de B é [illegible]. A probabilidade p_2 de escolher uma pedra azul de A e uma vermelha de B é [illegible] $= \frac{9}{40}$. Logo, $p = p_1 + p_2 =$ [illegible]

7.22 Demonstre: Se A e B são eventos independentes, então A^c e B^c são independentes.

Sejam $P(A) = x$ e $P(B) = y$. Então $P(A^c) = 1 - x$ e $P(B^c) = 1 - y$. Como A e B são independentes, $P(A \cap B) = P(A)P(B) = xy$. Além disso,

$$P(A \cup B) = P(A) + P(B) - P(A \cup B) = x + y - xy$$

Pela Lei de DeMorgan, $(A \cup B)^c = A^c \cap B^c$; logo,

$$P(A^c \cap B^c) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - x - y + xy$$

Por outro lado,

$$P(A^c)P(B^c) = (1 - x)(1 - y) = 1 - x - y + xy$$

Assim, $P(A^c \cap B^c) = P(A^c)P(B^c)$ e, portanto, A^c e B^c são independentes.

De maneira semelhante podemos mostrar que A e B^c, assim como A^c e B, são independentes.

Tentativas repetidas, distribuição binomial

7.23 Suponha que, sempre que os cavalos a, b, c e d correm juntos, suas respectivas probabilidades de vencer são 0,2, 0,5, 0,1 e 0,2. Ou seja, $S = \{a, b, c, d\}$, onde $P(a) = 0{,}2$, $P(b) = 0{,}5$, $P(c) = 0{,}1$ e $P(d) = 0{,}2$. Eles correm três vezes.

(*a*) Descreva e encontre o número de elementos no espaço de probabilidade S_3.

(*b*) Encontre a probabilidade de que o mesmo cavalo vença as três corridas.

(*c*) Encontre a probabilidade de que a, b e c vençam, cada um, uma corrida.

Por conveniência de notação, escrevemos xyz para (x, y, z).

(*a*) Por definição, $S_3 = S \times S \times S = \{xyz \mid x, y, z \in S\}$ e $P(xyz) = P(x)P(y)P(z)$.

Assim, em particular, S_3 contém $4^3 = 64$ elementos.

(*b*) Procuramos pela probabilidade do evento $A = \{aaa, bbb, ccc, ddd\}$. Por definição,

$$P(aaa) = (0{,}2)^3 = 0{,}008,\ P(ccc) = (0{,}1)^3 = 0{,}001$$
$$P(bbb) = (0{,}5)^3 = 0{,}125,\ P(ddd) = (0{,}2)^3 = 0{,}008$$

Portanto, $P(A) = 0{,}0008 + 0{,}125 + 0{,}001 + 0{,}008 = 0{,}142$.

(*c*) Procuramos pela probabilidade do evento $B = \{abc, acb, bac, bca, cab, cba\}$. Cada elemento de B tem a mesma probabilidade, o produto $(0{,}2)(0{,}5)(0{,}1) = 0{,}01$. Assim, $P(B) = 6(0{,}01) = 0{,}06$.

7.24 A probabilidade de que João acerte em um alvo é $p = \frac{1}{4}$. Ele atira $n = 6$ vezes. Encontre a probabilidade de que ele acerte no alvo: (*a*) exatamente duas vezes, (*b*) mais de quatro vezes; (*c*) pelo menos uma vez.

Esse é um experimento binomial com $n = 6$, $p = \frac{1}{4}$ e $q = 1 - p = \frac{3}{4}$, isto é, $B(6, \frac{1}{4})$. Consequentemente, empregamos o Teorema 7.7.

(*a*) $P(2) = \binom{6}{2}\left(\frac{1}{4}\right)^2\left(\frac{3}{4}\right)^4 = 15(3^4)/(4^6) = \frac{1215}{4096} \approx 0{,}297$

(*b*) $P(5) + P(6) = \binom{6}{5}\left(\frac{1}{4}\right)^5\left(\frac{3}{4}\right)^1 + \left(\frac{1}{4}\right)^6 = \frac{18}{4}^6 + \frac{1}{4}^6 = \frac{19}{4}^6 = \frac{19}{4096} \approx 0{,}0046$.

(*c*) $P(0) = \left(\frac{3}{4}\right)^6 = \frac{729}{4096}$, logo $P(X > 0) = 1 - \frac{729}{4096} = \frac{3367}{4096} \approx 0{,}82$.

7.25 Uma família tem seis crianças. Encontre a probabilidade p de que existam: (*a*) três meninos e três meninas, (*b*) menos meninos do que meninas. Considere que a probabilidade de qualquer criança ser um menino é $\frac{1}{2}$.

Aqui $n = 6$ e $p = q = \frac{1}{2}$

(*a*) $p = P(3\text{ meninos}) = \binom{6}{3}\left(\frac{1}{2}\right)^3\left(\frac{1}{2}\right)^3 = \frac{20}{64} = \frac{5}{16}$

(*b*) Há menos meninos do que meninas se existirem zero, um ou dois meninos. Logo,

$$p = P(0\text{ meninos}) + P(1\text{ menino}) + P(2\text{ meninos}) = \left(\frac{1}{2}\right)^6 + \binom{6}{1}\left(\frac{1}{2}\right)\left(\frac{1}{2}\right)^5 + \binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4 = \frac{11}{32} \approx 0{,}34$$

7.26 Um homem dispara em um alvo $n = 6$ vezes e o acerta $k = 2$ vezes. (*a*) Liste as diferentes maneiras como isso pode acontecer; (*b*) Quantas maneiras existem?

(*a*) Liste todas as sequências com dois S's (sucessos) e quatro F's (fracassos):

SSFFFF, SFSFFF, SFFSFF, SFFFSF, SFFFFS, FSSFFF, FSFSFF, FSFFSF,
FSFFFS, FFSSFF, FFSFSF, FFSFFS, FFFSSF, FFFSFS, FFFFSS.

(*b*) Há 15 maneiras diferentes, como indicado pela lista. Observe que isso é igual a $\binom{6}{2}$, pois estamos distribuindo $k = 2$ letras entre as $n = 6$ posições da sequência.

7.27 Demonstre o Teorema 7.7: A probabilidade de exatamente k sucessos em um experimento binomial $B(n, p)$ é dada por

$$P(k) = p(k \text{ sucessos}) = \binom{n}{k} p^k q^{n-k}$$

A probabilidade de um ou mais sucessos é $1 - q^n$.

O espaço amostral das n tentativas repetidas consiste em todas as n-uplas (isto é, sequências de n elementos) cujas componentes são S (sucessos) ou F (fracassos). Seja A o evento de exatamente k sucessos. Então A consiste em todas as n-uplas das quais k componentes são S, e $n - k$ componentes são F. O número de tais n-uplas no evento A é igual ao número de maneiras que k letras S podem ser distribuídas entre as n componentes de uma n-upla, logo, A consiste em $C(n, k) = \binom{n}{k}$ pontos amostrais. A probabilidade de cada ponto em A é $p^k q^{n-k}$; portanto,

$$P(A) = \binom{n}{k} p^k q^{n-k}$$

Especificamente, a probabilidade de nenhum sucesso é

$$P(0) = \binom{n}{0} p^0 q^n = q^n$$

Logo, a probabilidade de um ou mais sucessos é $1 - q^n$.

Variáveis aleatórias, valor esperado

7.28 Um apostador joga duas moedas justas. Ele ganha \$2 se ocorrerem duas caras e \$1 se ocorrer uma cara. Por outro lado, ele perde \$3 se nenhuma cara aparecer. Encontre o valor esperado E do jogo. Este jogo é justo? (O jogo é justo, favorável ou desfavorável para o jogador dependendo de $E = 0$, $E > 0$ ou $E < 0$.)

O espaço amostral $S = \{AA, AO, OA, OO\}$ e cada ponto amostral tem probabilidade 1/4. Para o ganho do jogador, temos

$$X(AA) = \$2, \qquad X(AO) = X(OA) = \$1, \qquad X(OO) = -\$3$$

Logo, a distribuição de X é o que se segue:

x	2	1	−3
p	1/4	2/4	1/4

Portanto, $E = E(X) = 2(1/4) + 1(2/4) - 3(1/4) = \$0{,}25$. Como $E(X) > 0$, o jogo é favorável ao apostador.

7.29 Você venceu um concurso. Seu prêmio é escolher um, de três envelopes, e ficar com o que está dentro dele. Cada um, entre dois envelopes, contém um cheque de \$30, mas o terceiro tem um cheque de \$3000. Encontre o valor esperado E de seus ganhos (como uma distribuição de probabilidades).

Seja X os seus ganhos. Então $X = 30$ ou 3000, e $P(30) = \frac{2}{3}$ e $P(3000) = \frac{1}{3}$. Logo,

$$E = E(X) = 30 \cdot \tfrac{2}{3} + 3000 \cdot \tfrac{1}{3} = 20 + 1000 = 1020$$

7.30 Uma amostra aleatória com relocação de tamanho $n = 2$ é tirada do conjunto $\{1, 2, 3\}$, conduzindo ao seguinte espaço amostral equiprovável de 9 elementos.

$$S = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

(*a*) Seja X a soma dos dois números. Encontre a distribuição f de X e o valor esperado de $E(X)$.

(*b*) Seja Y o mínimo entre os dois números. Encontre a distribuição g de X e o valor esperado $E(Y)$.

(*a*) A variável aleatória X assume os valores 2, 3, 4, 5 e 6. Calculamos a distribuição f de X:

(i) O ponto (1,1) tem soma 2; logo, $f(2)=\frac{1}{9}$.

(ii) Dois pontos, (1,2), (2,1), têm soma 3; logo, $f(3)=\frac{2}{9}$.

(iii) Três pontos, (1,3), (2,2), (3,1), têm soma 4; logo, $f(4)=\frac{3}{9}$.

(iv) Dois pontos, (2,3), (3,2), têm soma 5, logo, $f(5)=\frac{2}{9}$.

(v) O ponto (3,3) tem soma 6; logo, $f(6)=\frac{1}{9}$.

Assim, a distribuição f de X é:

x	2	3	4	5	6
$f(x)$	1/9	2/9	3/9	2/9	1/9

O valor esperado $E(X)$ de X é obtido multiplicando cada valor de x por sua probabilidade $f(x)$ e fazendo a soma. Portanto,

$$E(X)=2\left(\frac{1}{9}\right)+3\left(\frac{2}{9}\right)+4\left(\frac{3}{9}\right)+5\left(\frac{2}{9}\right)+6\left(\frac{1}{9}\right)=4$$

(*b*) A variável aleatória Y assume apenas os valores 1, 2 e 3. Calculamos a distribuição g de Y:

(i) Cinco pontos, (1,1), (1,2), (1,3), (2,1), (3,1), têm mínimo 1; logo, $g(1)=\frac{5}{9}$.

(ii) Três pontos, (2,2), (2,3), (3,2), têm mínimo 2; logo, $g(2)=\frac{3}{9}$.

(iii) O ponto (3,3) tem mínimo 3; Logo, $g(3)=\frac{1}{9}$.

Assim, o que se segue é a distribuição g de Y:

x	1	2	3
$g(x)$	5/9	3/9	1/9

O valor esperado $E(Y)$ de Y é:

$$E(Y)=1\left(\frac{5}{9}\right)+2\left(\frac{3}{9}\right)+3\left(\frac{1}{9}\right)=\frac{12}{9}\approx 1{,}33$$

7.31 Uma sequência finita linear EMPLOYEE tem n elementos. Suponha que NAME apareça aleatoriamente na sequência, e que existe uma busca linear para encontrar a localização K de NAME, ou seja, para encontrar K de modo que EMPLOYEE[K] = NAME. Seja $f(n)$ o número de comparações na busca linear.

(*a*) Encontre o valor esperado de $f(n)$.

(*b*) Encontre o valor máximo (pior caso) de $f(n)$.

(*a*) Seja X o número de comparações. Como NAME pode ocorrer em qualquer posição da sequência finita com a mesma probabilidade de $1/n$, temos $X=1,2,3,\ldots,n$, cada um com probabilidade $1/n$. Logo,

$$\begin{aligned} f(n)=E(X) &= 1\cdot\frac{1}{n}+2\cdot\frac{1}{n}+3\cdot\frac{1}{n}+\cdots+n\cdot\frac{1}{n} \\ &= (1+2+\cdots+n)\cdot\frac{1}{n}=\frac{n(n+1)}{2}\cdot\frac{1}{n}=\frac{n+1}{2} \end{aligned}$$

(*b*) Se NAME ocorrer no final da sequência finita, então $f(n)=n$.

Média, variância, desvio padrão

7.32 Encontre a média $\mu=E(X)$, variância $\sigma^2=Var(X)$ e desvio padrão $\sigma=\sigma_X$ de cada distribuição

(*a*)

x_i	2	3	11
p_i	1/3	1/2	1/6

(*b*)

x_i	1	3	4	5
p_i	0,4	0,1	0,2	0,3

Use as fórmulas

$$\mu=E(X)=x_1p_1+x_2p_2+\cdots+x_mp_m=\Sigma x_ip_i,\quad \sigma^2=Var(X)=E(X^2)-\mu^2$$

$$E(X^2)=x_1^2p_1+x_2^2p_2+\cdots+x_m^2p_m=\Sigma x_i^2p_i,\qquad \sigma=\sigma_x=\sqrt{Var(X)}$$

(*a*) $\mu = \Sigma x_i p_i = 2(\frac{1}{3}) + 3(\frac{1}{2}) + 11(\frac{1}{6}) = 4$
$E(X^2) = \Sigma x_i^2 p_i = 2^2(\frac{1}{3}) + 3^2(\frac{1}{2}) + 11^2(\frac{1}{6}) = 26$
$\sigma^2 = Var(X) = E(X^2) - \mu^2 = 26 - 4^2 = 10$
$\sigma = \sqrt{Var(X)} = \sqrt{10} = 3{,}2$

(*b*) $\mu = \Sigma x_i p_i = 1(0{,}4) + 3(0{,}1) + 4(0{,}2) + 5(0{,}3) = 3$
$E(X^2) = \Sigma x_i^2 p_i = 1(0{,}4) + 9(0{,}1) + 16(0{,}2) + 25(0{,}3) = 12$
$\sigma^2 = Var(X) = E(X^2) - \mu^2 = 12 - 9 = 3$
$\sigma = \sqrt{Var(X)} = \sqrt{3} = 1{,}7$

7.33 Um dado justo é jogado, conduzindo ao espaço amostral equiprovável $S = \{1, 2, 3, 4, 5, 6\}$, onde $n(S) = 6$ e cada ponto tem probabilidade $1/6$.

(*a*) Seja X a variável aleatória que denota o dobro do número que ocorre. Encontre a distribuição f de X e seu valor esperado $E(X)$.

(*b*) Seja Y a variável aleatória que assinala 1 ou 3, dependendo de ocorrer um número ímpar ou par. Encontre a distribuição g de Y e seu valor esperado $E(Y)$.

(*a*) Aqui o espaço imagem $R_X = \{2, 4, 6, 8, 10, 12\}$, uma vez que

$$X(1) = 2, \quad X(2) = 4, \quad X(3) = 6, \quad X(4) = 8, \quad X(5) = 10, \quad X(6) = 12$$

Além disso, cada número ocorre com probabilidade $1/6$. Assim, a distribuição f de X se segue

x	2	4	6	8	10	12
$f(x)$	1/6	1/6	1/6	1/6	1/6	1/6

Portanto,

$$E(X) = \sum x f(x) = \frac{2}{6} + \frac{4}{6} + \frac{6}{6} + \frac{8}{6} + \frac{10}{6} + \frac{12}{6} = 7$$

(*b*) Aqui o espaço imagem $R_Y = \{1, 3\}$, pois

$$Y(1) = 1, Y(2) = 3, Y(3) = 1, Y(4) = 3, Y(5) = 1, Y(6) = 3$$

Calculamos a distribuição g de Y usando o fato de que $n(S) = 6$:

(i) Três pontos, 1, 3, 5, são ímpares e têm imagem 1, logo, $g(1) = 3/6$.

(ii) Três pontos, 2, 4, 6, são pares e têm imagem 3, logo, $g(3) = 3/6$.

Assim, a distribuição g de Y é:

y	1	3
$g(y)$	3/6	3/6

Portanto,

$$E(Y) = \sum y g(y) = \frac{3}{6} + \frac{9}{6} = 2$$

7.34 Seja $Z = X + Y$, onde X e Y são as variáveis aleatórias do Problema 7.33. Encontre a distribuição h de Z e determine $E(Z)$. Verifique que $E(X + Y) = E(X) + E(Y)$.

O espaço amostral ainda é $S = \{1, 2, 3, 4, 5, 6\}$ e cada ponto ainda tem probabilidade $1/6$. Obtemos, usando $Z(s) = (X + Y)(s) = X(s) + Y(s)$,

$$Z(1) = X(1) + Y(1) = 2 + 1 = 3, \quad Z(4) = X(4) + Y(4) = 8 + 3 = 11,$$
$$Z(2) = X(2) + Y(2) = 4 + 3 = 7, \quad Z(5) = X(5) + Y(5) = 10 + 1 = 11,$$
$$Z(3) = X(3) + Y(3) = 6 + 1 = 7, \quad Z(6) = X(6) + Y(6) = 12 + 3 = 15$$

Assim, o espaço imagem $R_Z = \{3, 7, 11, 15\}$. Computamos a distribuição h de Z, usando o fato de que $n(S) = 6$.

(i) Um ponto tem imagem 3, logo, $h(3) = 1/6$. (iii) Dois pontos têm imagem 11; logo, $h(11) = 2/6$.

(ii) Dois pontos têm imagem 7, logo, $h(7) = 2/6$. (iv) Um ponto tem imagem 15; logo, $h(15) = 1/6$.

Assim, a distribuição h de Z é o que se segue

z	3	7	11	15
$h(z)$	1/6	2/6	2/6	1/6

Logo,

$$E(Z) = \sum z h(z) = \frac{3}{6} + \frac{14}{6} + \frac{22}{6} + \frac{15}{6} = 9$$

Consequentemente,

$$E(X + Y) = E(Z) = 9 = 7 + 2 = E(X) + E(Y)$$

Distribuição binomial

7.35 A probabilidade de que um homem atinja um alvo é $p = 0{,}1$. Ele dispara $n = 100$ vezes. Encontre o valor esperado μ de vezes que ele atinge o alvo e o desvio padrão σ.

Esse é um experimento binomial $B(n, p)$, onde $n = 100$, $p = 0{,}1$ e $q = 1 - p = 0{,}9$. Portanto, aplicamos o Teorema 7.9 para obter

$$\mu = np = 100(0{,}1) = 10 \quad \text{e} \quad \sigma = \sqrt{npq} = \sqrt{100(0{,}1)(0{,}9)} = 3$$

7.36 Um estudante realiza uma prova de múltipla escolha com 18 questões, a qual apresenta quatro opções por questão. Suponha que uma das opções é obviamente incorreta, e que o estudante faça uma adivinhação "pensa" dentre demais. Encontre o número esperado $E(X)$ de respostas corretas e o desvio padrão σ.

Esse é um experimento binomial $B(n, p)$, onde $n = 18$, $p = \frac{1}{3}$ e $q = 1 - p = \frac{2}{3}$. Logo,

$$E(X) = np = 18 \cdot \tfrac{1}{3} = 6 \quad \text{e} \quad \sigma = \sqrt{npq} = \sqrt{18 \cdot \tfrac{1}{3} \cdot \tfrac{2}{3}} = 2$$

7.37 A função de valor esperado $E(X)$ sobre o espaço de variáveis aleatórias em um espaço amostral S pode ser provada como sendo *linear*, isto é,

$$E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$$

Use essa propriedade para demonstrar que $\mu = np$ para um experimento binomial $B(n, p)$.

No espaço amostral de n tentativas de Bernoulli, seja X_i (para $i = 1, 2, \ldots, n$) uma variável aleatória que tem o valor 1 ou 0, dependendo da i-ésima tentativa ser um sucesso ou um fracasso. Então, cada X_i tem a distribuição

x	0	1
$p(x)$	q	p

Assim, $E(X_i) = 0(q) + 1(p) = p$. O número total de sucessos em n tentativas é

$$X = X_1 + X_2 + \cdots + X_n$$

Usando a propriedade de linearidade de E, temos

$$\begin{aligned} E(X) &= E(X_1 + X_2 + \cdots + X_n) \\ &= E(X_1) + E(X_2) + \cdots + E(X_n) \\ &= p + p + \cdots + p = np \end{aligned}$$

Problemas variados

7.38 Suponha que X é uma variável aleatória com média $\mu = 75$ e desvio padrão $\sigma = 5$. Estime a probabilidade que X se encontre entre $75 - 20 = 55$ e $75 + 20 = 95$.

Lembre que a Desigualdade de Chebyshev estabelece que

$$P(\mu - k\sigma \leq X \leq \mu + k\sigma) \geq 1 - \frac{1}{k^2}$$

Aqui $k\sigma = 20$. Como $\sigma = 5$, obtemos $k = 4$. Então, pela Desigualdade de Chebyshev,

$$P(55 \leq X \leq 95) \geq 1 - \frac{1}{4^2} = \frac{15}{16} \approx 0{,}94$$

7.39 Seja X uma variável aleatória com média $\mu = 40$ e desvio padrão $\sigma = 2$. Use a Desigualdade de Chebyshev para encontrar um b para o qual $P(40 - b \leq X \leq 40 + b) \geq 0{,}95$.

Primeiro isole k em $1 - 1/k^2 = 0{,}95$ como se segue:

$$0{,}05 = \frac{1}{k^2} \quad \text{ou} \quad k^2 = \frac{1}{0{,}05} = 20 \quad \text{ou} \quad k = \sqrt{20} = 2\sqrt{5}$$

Então, pela Desigualdade de Chebyshev, $b = k\sigma = 10\sqrt{5} \approx 23{,}4$. Logo, $[P(16{,}6 \leq X \leq 63{,}60) \geq 0{,}95]$

7.40 Seja X uma variável aleatória com distribuição f. O r-ésimo *momento* M_r de X é definido por

$$M_r = E(X^r) = \sum x_i^r f(x_i)$$

Encontre os quatro primeiros momentos de X se X tem a distribuição:

x	-2	1	3
$f(x)$	$1/2$	$1/4$	$1/4$

Observe que M_1 é a média de X, e M_2 é usado para calcular o desvio padrão de X.

Use a fórmula de M_r para obter:

$$M_1 = \sum x_i f(x_i) = -2\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{4}\right) + 3\left(\tfrac{1}{4}\right) = 0$$
$$M_2 = \sum x_i^2 f(x_i) = 4\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{4}\right) + 9\left(\tfrac{1}{4}\right) = 4{,}5$$
$$M_3 = \sum x_i^3 f(x_i) = -8\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{4}\right) + 27\left(\tfrac{1}{4}\right) = 3$$
$$M_4 = \sum x_i^4 f(x_i) = 16\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{4}\right) + 81\left(\tfrac{1}{4}\right) = 28{,}5$$

7.41 Demonstre o Teorema 7.10 (Desigualdade de Chebyshev): Para $k > 0$,

$$P(\mu - k\sigma \leq X \leq \mu + k\sigma) \geq 1 - \frac{1}{k^2}$$

Por definição,

$$\sigma^2 = \mathrm{Var}(X) = \sum (x_i - \mu)^2 p_i$$

Elimine todos os termos do somatório para os quais x_i está no intervalo $[\mu - k\sigma, \mu + k\sigma]$, ou seja, elimine todos os termos para os quais $|x_i - \mu| \leq k\sigma$. Denote o somatório dos termos restantes por $\sum^* (x_i - \mu)^2 p_i$. Então,

$$\left[\sigma^2 \geq \sum{}^* (x_i - \mu)^2 p_i \geq \sum{}^* k^2\sigma^2 p_i = k^2\sigma^2 \sum{}^* p_i = k^2\sigma^2 P(|X - \mu| > k\sigma)\right]$$
$$= k^2\sigma^2[1 - P(|X - \mu| \leq k\sigma)] = k^2\sigma^2[1 - P(\mu - k\sigma \leq X \leq \mu + k\sigma)]$$

Se $\sigma > 0$, então dividindo por $k^2\sigma^2$, temos

$$\frac{1}{k^2} \geq 1 - P(\mu - k\sigma \leq X \leq \mu + k\sigma) \quad \text{ou} \quad P(\mu - k\sigma \leq X \leq \mu + k\sigma) \geq 1 - \frac{1}{k^2}$$

o que prova a Desigualdade de Chebyshev para $\sigma > 0$. Se $\sigma = 0$, então $x_i = \mu$ para todo $p_i > 0$, e

$$P(\mu - k \cdot 0 \leq X \leq \mu + k \cdot 0) = P(X = \mu) = 1 > 1 - \frac{1}{k^2}$$

o que completa a demonstração.

Problemas Complementares

Espaços amostrais e eventos

7.42 Sejam A, B e C eventos. Reescreva cada um dos eventos a seguir, usando notação conjuntista:

(a) A e B ocorrem, mas não C; (c) nenhum dos eventos ocorre;

(b) A ou C ocorrem, mas não B; (d) pelo menos dois dos eventos ocorrem.

7.43 Uma moeda de um centavo, uma moeda de dez centavos e um dado são jogados.

(a) Descreva um espaço amostral S adequado e determine $n(S)$.

(b) Escreva explicitamente os seguintes eventos:

A = {duas caras e um número par}

B = {2 ocorre}

C = {exatamente uma cara e um número ímpar}

(c) Escreva explicitamente os eventos: (i) A e B; (ii) apenas B; (iii) B e C.

7.44 Determine a probabilidade de cada evento:

(a) Um número ímpar ocorre no jogo de um dado justo.

(b) Uma ou mais caras ocorrem no jogo de quatro moedas justas.

(c) Um ou mais números excedem 4 no jogo de dois dados justos.

7.45 Um cartão é escolhido aleatoriamente de 50 cartões numerados de 1 a 50. Encontre a probabilidade de que o número do cartão é

(a) maior do que 10; (c) maior do que 10 e divisível por 5;

(b) divisível por 5; (d) maior do que 10 ou divisível por 5.

7.46 Entre 10 garotas de uma turma, três têm olhos azuis. Duas das garotas são escolhidas aleatoriamente. Encontre a probabilidade de que:

(a) ambas tenham olhos azuis; (c) pelo menos uma tenha olhos azuis;

(b) nenhuma tenha olhos azuis; (d) exatamente uma tenha olhos azuis.

7.47 Dez estudantes A, B, ..., estão em uma turma. Um comitê de três é escolhido aleatoriamente para representar a turma. Encontre a probabilidade de que:

(a) A pertença ao comitê; (c) A e B pertençam ao comitê;

(b) B pertença ao comitê; (d) A ou B pertençam ao comitê.

7.48 Três parafusos e três porcas estão em uma caixa. Dois objetos são escolhidos aleatoriamente. Determine a probabilidade de que um é parafuso e outro é uma porca.

7.49 Uma caixa contém duas meias brancas, duas azuis e duas vermelhas. Duas meias são retiradas aleatoriamente. Encontre a probabilidade de que elas casem (tenham a mesma cor).

7.50 Entre 120 alunos, 60 estudam francês, 50 estudam espanhol e 20 estudam francês e espanhol. Um estudante é escolhido aleatoriamente. Encontre a probabilidade de que ele estude: (a) francês ou espanhol, (b) nem francês, nem espanhol, (c) apenas francês; (d) exatamente um dos dois idiomas.

Espaços finitos de probabilidades

7.51 Decida quais das seguintes funções definem um espaço de probabilidades sobre $S = \{a_1, a_2, a_3\}$

(a) $P(a_1) =$ [illegible], $P(a_2) =$ [illegible], $P(a_3) =$ [illegible]   (c) $P(a_1) =$ [illegible], $P(a_2) =$ [illegible], $P(a_3) =$ [illegible]

(b) $P(a_1) =$ [illegible], $P(a_2) =$ [illegible], $P(a_3) = \frac{2}{3}$ (d) $P(a_1) = 0$, $P(a_2) =$ [illegible], $P(a_3) =$ [illegible]

7.52 Uma moeda é viciada, de modo que cara é três vezes mais provável de ocorrer do que coroa. Determine $P(A)$ e $P(O)$.

7.53 Três alunos, A, B e C, estão em uma competição de natação. A e B têm a mesma probabilidade de vencer, e cada um deles tem o dobro de chances de vencer C. Encontre a probabilidade de que: (a) B vença; (b) C vença, (c) B ou C vençam.

7.54 Considere a seguinte distribuição de probabilidades:

Resultado x	1	2	3	4	5
Probabilidade $P(x)$	0,2	0,4	0,1	0,1	0,2

Considere os eventos $A = \{\text{número par}\}$, $B = \{2, 3, 4, 5\}$, $C = \{1, 2\}$. Encontre:

(a) $P(A)$, $P(B)$, $P(C)$; (b) $P(A \cap B)$, $P(A \cap C)$, $P(B \cap C)$.

7.55 Suponha que A e B são eventos com $P(A) = 0{,}7$, $P(B) = 0{,}5$ e $P(A \cap B) = 0{,}4$. Encontre a probabilidade de que:

(a) A não ocorra; (c) A ocorra, mas B não;

(b) A ou B ocorram, (d) nem A, nem B ocorram.

Probabilidade condicional, independência

7.56 Um dado justo é lançado. Considere os eventos $A = \{2, 4, 6\}$, $B = \{1, 2\}$ e $C = \{1, 2, 3, 4\}$. Encontre:

(a) $P(A \text{ e } B)$ e $P(A \text{ ou } C)$; (c) $P(A|C)$ e $P(C|A)$;

(b) $P(A|B)$ e $P(B|A)$; (d) $P(B|C)$ e $P(C|B)$.

Decida quais das seguintes são independentes: (i) A e B; (ii) A e C; (iii) B e C.

7.57 Um par de dados é jogado. Se os números que aparecem são distintos, encontre a probabilidade de que: (a) a soma é par; (b) a soma exceda nove.

7.58 Sejam A e B eventos com $P(A) = 0{,}6$, $P(B) = 0{,}3$ e $P(A \cap B) = 0{,}2$. Encontre:

(a) $P(A \cup B)$; (b) $P(A|B)$; (c) $P(B|A)$.

7.59 Sejam A e B eventos com $P(A) = 1/3$, $P(B) = \frac{1}{4}$ e $P(A \cup B) =$ [illegible].

(a) Determine $P(A|B)$ e $P(B|A)$; (b) A e B são independentes?

7.60 Sejam A e B eventos com $P(A) = 0{,}3$, $P(A \cup B) = 0{,}5$ e $P(B) = p$. Determine p se:

(a) A e B são mutuamente disjuntos, (b) A e B são independentes, (c) A é subconjunto de B

7.61 Sejam A e B eventos independentes com $P(A) = 0{,}3$ e $P(B) = 0{,}4$. Encontre:

(a) $P(A \cap B)$ e $P(A \cup B)$; (b) $P(A|B)$ e $P(B|A)$.

7.62 Em um clube, 60% das mulheres jogam tênis, 40% jogam golfe e 20% jogam tênis e golfe. Uma mulher é escolhida aleatoriamente.

(a) Determine a probabilidade de que ela não jogue tênis nem golfe.

(b) Se ela joga tênis, encontre a probabilidade de que ela jogue golfe.

(c) Se ela joga golfe, determine a probabilidade de que ela jogue tênis.

7.63 A caixa A contém seis pedras vermelhas e duas azuis, e a caixa B contém duas pedras vermelhas e quatro azuis. Uma pedra é retirada aleatoriamente de cada caixa.

(a) Encontre a probabilidade p de que ambas as pedras são vermelhas.

(b) Determine a probabilidade p de que uma é vermelha e outra é azul.

7.64 A probabilidade de que A atinja um alvo é $\frac{1}{[illegible]}$, e a probabilidade de que B atinja o alvo é [illegible].

(a) Se cada um dispara duas vezes, qual é a probabilidade de que o alvo seja atingido pelo menos uma vez?

(b) Se cada um dispara uma vez, e o alvo é atingido apenas uma vez, qual é a probabilidade de que A acertou no alvo?

7.65 Três moedas justas são jogadas. Considere os eventos

$A = \{$todas caras ou todas coroas$\}$, $B = \{$pelo menos duas caras$\}$, $C = \{$duas caras no máximo$\}$

Entre os pares (A, B), (A, C) e (B, C), quais são independentes? Quais são dependentes?

7.66 Determine $P(B|A)$ se: (a) A é um subconjunto de B; (b) A e B são mutuamente exclusivos. (Assuma que $P(A) > 0$.)

Tentativas repetidas, distribuição binomial

7.67 Sempre que os cavalos a, b e c correm juntos, suas respectivas probabilidades de vencer são 0,3, 0,5 e 0,2. Eles correm três vezes.

(a) Encontre a probabilidade de que o mesmo cavalo vença todas as corridas.

(b) Encontre a probabilidade de que a, b e c vençam, cada um, uma corrida.

7.68 A média de batidas de um jogador de beisebol é 0,300. Ele entra para bater quatro vezes. Encontre a probabilidade de que ele consiga: (a) exatamente duas batidas; (b) pelo menos uma batida.

7.69 A probabilidade de que Tom acerte uma jogada de três pontos de basquetebol é $p = 0{,}4$. Ele joga $n = 5$ vezes. Encontre a probabilidade de que ele acerte: (a) exatamente duas vezes; (b) pelo menos uma vez.

7.70 Um certo tipo de míssil atinge seu alvo com probabilidade $P = \frac{1}{[illegible]}$.

(a) Se três mísseis são disparados, determine a probabilidade de que o alvo seja atingido pelo menos uma vez.

(b) Encontre o número de mísseis que devem ser disparados, de modo que exista uma probabilidade de pelo menos 90% de acertar no alvo.

Variáveis aleatórias

7.71 Um par de dados é jogado. Seja X o menor dos dois números que ocorrem. Encontre a distribuição e o valor esperado de X.

7.72 Uma moeda não viciada é jogada quatro vezes. Seja X a mais longa sequência de caras. Encontre a distribuição e o valor esperado de X.

7.73 Uma moeda não viciada é jogada até que uma cara ou cinco coroas ocorram. Encontre o número esperado E de jogadas da moeda.

7.74 Uma moeda é viciada, de modo que $P(A) = \frac{3}{4}$ e $P(O) = \frac{1}{4}$. A moeda é jogada três vezes. Seja X o número de caras que aparecem.

(a) Encontre a distribuição f de X. (b) Encontre o valor esperado $E(X)$.

7.75 A probabilidade do time A vencer qualquer jogo é [illegible] Suponha que A joga contra B em um torneio. O primeiro time a vencer dois jogos seguidos, ou três partidas, vence o torneio. Determine o número esperado de jogos no torneio.

7.76 Uma caixa contém 10 transistores, dos quais dois são defeituosos. Cada transistor é escolhido e testado até que um não defeituoso seja selecionado. Determine o número esperado de transistores a serem escolhidos.

7.77 Uma loteria com 500 bilhetes dá um prêmio de \$100, três prêmios de \$50 cada, e cinco prêmios de \$25 cada.

(a) Determine as premiações esperadas de um bilhete. (b) Se um bilhete custa \$1, qual é o valor esperado do jogo?

7.78 Um apostador joga três moedas não viciadas. Ele ganha \$5 se três caras ocorrerem, \$3 se duas caras ocorrerem, e \$1 se aparecer apenas uma cara. Por outro lado, ele perde \$15 se ocorrerem três coroas. Encontre o valor do jogo para o apostador.

Média, variância e desvio padrão

7.79 Determine a média μ, a variância σ^2 e o desvio padrão σ de cada distribuição:

(a)

x	2	3	8
$f(x)$	¼	½	¼

(b)

y	−1	0	1	2	3
$g(y)$	0,3	0,1	0,1	0,3	0,2

7.80 Encontre a média μ, a variância σ^2 e o desvio padrão σ da seguinte distribuição de dois pontos, onde $p + q = 1$

x	a	b
$f(x)$	p	q

7.81 Seja $W = XY$, onde X e Y são as variáveis aleatórias do Problema 7.33. (Lembre que $W(s) = (XY)(s) = X(s)Y(s)$.) Encontre: (a) a distribuição h de W; (b) $E(W)$.

Podemos afirmar que $E(W) = E(X)E(Y)$?

7.82 Seja X uma variável aleatória com a distribuição:

x	−1	1	2
$f(x)$	0,2	0,5	0,3

(a) Determine a média, a variância e o desvio padrão de X.

(b) Encontre a distribuição, a média, a variância e o desvio padrão de Y, onde:

(i) $Y = X^4$, (ii) $Y = 3^X$

Distribuição binomial

7.83 A probabilidade de que uma mulher acerte em um alvo é $p = 1/3$. Encontre o número esperado μ de vezes que ela acerte o alvo e o desvio padrão σ.

7.84 O time A tem probabilidade $p = 0,8$ de vencer cada vez que ele joga. Seja X o número de vezes que A vence em $n = 100$ jogos. Encontre a média μ, a variância σ^2 e o desvio padrão σ de X.

7.85 Um estudante despreparado faz um teste de cinco perguntas do tipo verdadeiro-falso e responde aleatoriamente cada questão. Determine a probabilidade de que o estudante seja aprovado no teste se pelo menos quatro questões corretas correspondem à nota mínima.

7.86 Seja X uma variável aleatória $B(n, p)$ distribuída binomialmente com $E(X) = 2$ e $Var(X) =$ [illegible]. Determine n e p.

Desigualdade de Chebyshev

7.87 Seja X uma variável aleatória com média μ e desvio padrão σ. Use a Desigualdade de Chebyshev para estimar $P(\mu - 3\sigma < X < \mu + 3\sigma)$.

7.88 Seja Z a variável aleatória com média $\mu = 0$ e desvio padrão $\sigma = 1$.

Use a Desigualdade de Chebyshev para encontrar um valor b para o qual $P(-b \leq Z \leq b) = 0,9$.

7.89 Seja X uma variável aleatória com média $\mu = 0$ e desvio padrão $\sigma = 1,5$.

Use a Desigualdade de Chebyshev para estimar $P(-3 \leq X \leq 3)$.

7.90 Seja X uma variável aleatória com média $\mu = 70$.

Para qual valor de σ a Desigualdade de Chebyshev fornece $P(65 \leq X \leq 75) \geq 0,95$?

Respostas dos Problemas Complementares

A notação $[x_1, \ldots, x_n; f(x_1), \ldots, f(x_n)]$ é usada para a distribuição $f = \{(x_i, f(X_i))\}$.

7.42 (a) $A \cap B \cap C^C$; (c) $(A \cup B \cup B)^C = A^C \cap B^C C^C$;

(b) $(A \cup C) \cap B^C$; (d) $(A \cap B) \cup (A \cap C) \cup (B \cap C)$

7.43 (a) $n(S) = 24$, $S = \{A, O\} \times \{A, O\} \times \{1, 2, \ldots, 6\}$
(b) $A = \{AA2, AA4, AA6\}$; $B = \{AA2, AO2, OA2, OO2\}$; $C = \{AO1, AO3, AO5, OA1, OA3, OA5\}$
(c) (i) $AA2$; (ii) $AO2, OA2, OO2$, (iii) $\varnothing$.

7.44 (a) 3/6; (b) 15/16; (c) 20/36.

7.45 (a) 40/50; (b) 10/50; (c) 8/50; (d) 42/50.

7.46 (a) 1/15, (b) 7/15; (c) 8/15; (d) 7/15.

7.47 (a) 3/10; (b) 3/10; (c) 1/15; (d) 8/15.

7.48 3/5.

7.49 1/5.

7.50 (a) 3/4; (b) 1/4; (c) 1/3, (d) 7/12.

7.51 (c) e (d).

7.52 $P(A) = 3/4$; $P(O) = 1/4$

7.53 (a) 2/5, (b) 1/5; (c) 3/5

7.54 (a) 0,6, 0,8, 0,5; (b) 0,5, 0,7, 0,4.

7.55 (a) 0,3; (b) 0,8; (c) 0,3, (d) 0,2.

7.56 (a) 1/6, 5/6; (b) 1/2, 1/3; (c) 1/2, 2/3; (d) 1/2, (i) sim; (ii) sim; (iii) não.

7.57 (a) 12/30; (b) 4/30.

7.58 (a) 0,7, (b) 2/3; (c) 1/3.

7.59 (a) 1/3, 1/4; (b) sim.

7.60 (a) 0,2; (b) 2/7; (c) 0,5.

7.61 (a) 0,12, 0,58, (b) 3/10, 4/10

7.62 (a) 20%; (b) 1/3; (c) 1/2.

7.63 (a) 1/4, (b) 7/12.

7.64 (a) 3/4; (b) 1/3.

7.65 Apenas A e B são independentes.

7.66 (a) 1, (b) 0.

7.67 (a) 0,16; (b) 0,18.

7.68 $6(0{,}3)^2(0{,}7)^2 = 0{,}2646$; (b) $1 - (0{,}7)^4 = 0{,}7599$

7.69 (a) $10(0{,}4)^2(0{,}6)^3$; (b) $1 - (0{,}6)^5$.

7.70 (a) $1 - (2/3)^5 = 211/243$; (b) seis vezes.

7.71 [1, 2, 3, 4, 5, 6; 11/36, 9/36, 7/36, 5/36, 3/36, 1/36],
$E(X) = 91/36 \approx 2{,}5$.

7.72 [0, 1, 2, 3, 4; 1/16, 7/16, 5/16, 2/16, 1/16],
$E(X) = 27/16 \approx 1{,}7$.

7.73 $E = 1{,}9$.

7.74 (a) [0, 1, 2, 3; 1/64, 9/64, 27/64, 27/64,; (b) $E(X) = 2{,}25$

7.75 $23/8 \approx 2{,}9$.

7.76 $11/9 \approx 1{,}2$.

7.77 (a) 0,75; (b) −0,25.

7.78 0,25.

7.79 (a) $\mu = 4$, $\sigma^2 = 5{,}5$, $\sigma = 2{,}3$, (b) $\mu = 1$, $\sigma^2 = 2{,}4$, $\sigma = 1{,}5$.

7.80 $\mu = ap + bq$, $\sigma^2 = pq(a - b)^2$, $\sigma = a - b\sqrt{pq}$

7.81 (a) [2, 6, 10, 12, 24, 36; 1/6, . . . , 1/6], (b) $E(W) = 15$. Não.

7.82 (a) 0,9, 1,09, 1,04; (b) (i) [1, 1, 16, 0,2, 0,5, 0,3], 5,5, 47,25, 6,87; (ii) [1/3, 3, 9; 0,2, 0,5, 0,3] 4,67, 5,21, 3,26.

7.83 $\mu = 50/3 = 16{,}67$, $\sigma = 10/3 = 3{,}33$.

7.84 $\mu = 80$; $\sigma^2 = 16$; $\sigma = 4$.

7.85 6/32.

7.86 $n = 6$, $p = 1/3$.

7.87 $P \geq 1 - 1/8 \approx 8{,}75$.

7.88 $b = \sqrt{10}\ 10 \approx 3{,}16$.

7.89 $P \geq 0{,}75$.

7.90 $\sigma = 5/\sqrt{20} \approx 1{,}12$.

Teoria dos Grafos

8.1 INTRODUÇÃO, ESTRUTURAS DE DADOS

Grafos, grafos orientados, árvores e árvores binárias aparecem em muitas áreas da matemática e da ciência da computação. Este e os próximos dois capítulos cobrem tais tópicos. Contudo, para entender como esses objetos podem ser armazenados em memória e para compreender algoritmos sobre eles, precisamos conhecer um pouco sobre certas estruturas de dados. Assumimos que o leitor compreenda arrays lineares e bidimensionais,† logo, discutimos a seguir apenas listas ligadas e apontadores (ou ponteiros), bem como pilhas e filas.

Listas ligadas e apontadores

Listas ligadas e apontadores são introduzidos por meio de um exemplo. Suponha que uma empresa de corretores mantenha um arquivo no qual cada registro contém um nome de cliente e vendedor; digamos que o arquivo contenha os seguintes dados:

Cliente	Adams	Brown	Clark	Drew	Evans	Farmer	Geller	Hiller	Infeld
Vendedor	Smith	Ray	Ray	Jones	Smith	Jones	Ray	Smith	Ray

Há duas operações básicas que podem ser executadas sobre os dados.

Operação A: Dado o nome de um cliente, determinar seu vendedor.

Operação B: Dado o nome de um vendedor, determinar a lista de seus clientes.

Discutimos várias maneiras de como os dados podem ser armazenados no computador e a facilidade com que se pode executar as operações A e B sobre os dados.

Claramente, o arquivo poderia ser armazenado no computador por um array com duas linhas (ou colunas) de nove nomes. Como os clientes são listados alfabeticamente, poderíamos facilmente executar a operação A. No entanto, para realizarmos a operação B, devemos buscar ao longo de todo o array.

Pode-se facilmente armazenar os dados na memória usando um array bidimensional no qual, digamos, as linhas correspondem a uma listagem alfabética dos clientes, e as colunas a uma listagem alfabética dos vendedores, e onde uma entrada 1 na matriz indica o vendedor de um cliente e os 0's ocupam as demais entradas. O principal problema de tal representação é que pode haver um desperdício de muita memória, pois muitos 0's podem estar na matriz. Por exemplo, se uma empresa tem 1000 clientes e 20 vendedores, seriam necessárias 20 000 locações de memória para os dados, mas apenas 1000 delas seriam úteis.

Discutimos abaixo uma maneira de armazenar os dados na memória, a qual usa listas ligadas e apontadores. Por uma *lista ligada* queremos dizer uma coleção linear de elementos de dados, onde a ordem linear é dada por meio de um *campo apontador*. A Fig. 8-1 é um diagrama esquemático de uma lista ligada com seis nós. Ou seja,

---

† N. de T.: Um array linear é comumente descrito como uma n-upla ordenada $(a_1, a_2, \ldots, a_n)$, enquanto um array bidimensional é simplesmente uma matriz.

cada nó é dividido em duas partes: a primeira contém a informação do elemento (por exemplo, NOME, ENDEREÇO,...), e a segunda parte, chamada de *campo de ligação* ou *campo apontador*, contém o endereço do próximo nó da lista. Esse campo apontador é indicado por uma flecha esboçada de um nó para o próximo na lista. Há também um apontador variável, chamado de START na Fig. 8-1, que fornece o endereço do primeiro nó na lista. Além disso, o campo apontador do último nó contém um endereço inválido, chamado de *apontador nulo*, o qual indica o fim da lista.

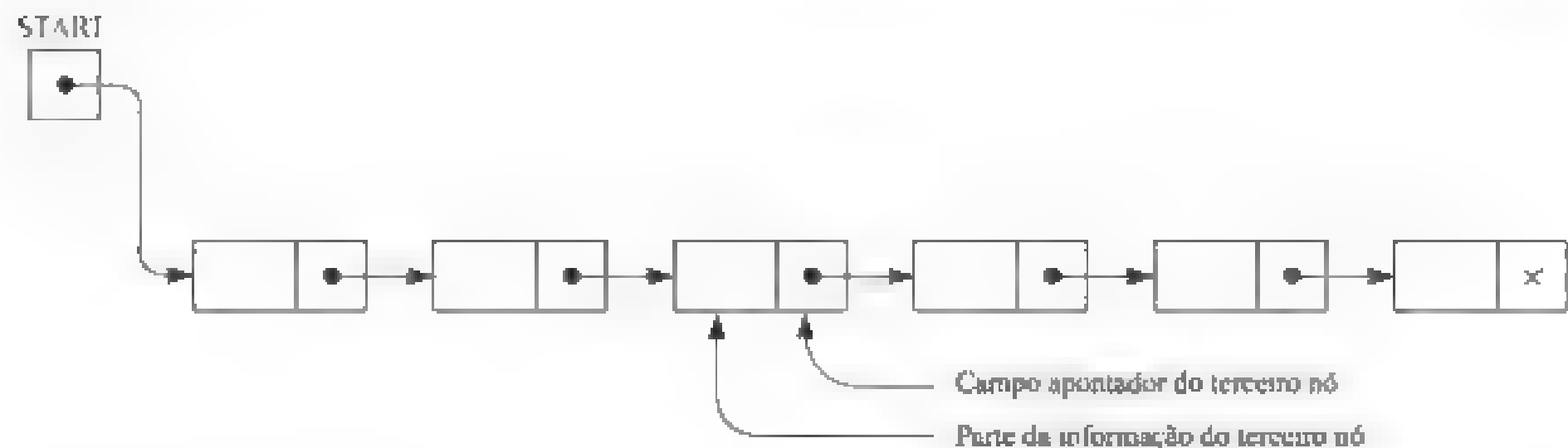



Figura 8-1 Lista ligada com 6 nós.

Uma maneira principal de armazenar os dados originais retratados na Fig. 8-2 usa listas ligadas. Observe que há arrays separados (arranjados alfabeticamente) para os clientes e para os vendedores. Além disso, existe um array apontador SLSM paralelo a CLIENTE que fornece a localização do vendedor de um cliente, logo, a operação *A* pode ser realizada com muita facilidade e rapidez. Também a lista de clientes de cada vendedor é uma lista ligada, como discutido acima. Especificamente, há um array apontador START paralelo a VENDEDOR, que aponta para o primeiro cliente de um vendedor, assim como um array NEXT que aponta para a localização do próximo cliente na lista do vendedor (ou contém um 0 para indicar o fim da lista). Esse processo é indicado pelas flechas na Fig. 8-2 para o vendedor Ray.

	Cliente	SLSM	NEXT
	Adams	3	5
2	Brown	2	3
3	Clark	2	7
4	Drew	1	6
5	Evans	3	8
6	Farmer	1	0
7	Geller	2	9
8	Hill	3	0
9	Infeld	2	0

Vendedor	START	
Jones	4	1
Ray	2	2
Smith	1	3

Figura 8-2

A operação *B* pode agora ser executada de modo fácil e rápido; ou seja, não é necessário buscar ao longo da lista de todos os clientes para obter a lista de clientes de um dado vendedor. A Fig. 8-3 nos dá um algoritmo (que é escrito em pseudocódigo).

Pilhas, filas e filas de prioridade

Existem outras estruturas de dados além de arrays e listas ligadas que devem ocorrer em nossos algoritmos gráficos. Estas estruturas, pilhas, filas e filas de prioridade, são brevemente descritas abaixo.

(a) **Pilhas**: Uma *pilha* (*stack*), também chamada de sistema "último a entrar é o primeiro a sair" (LIFO, na sigla em inglês para *last-in-first-out*), é uma lista linear na qual inserções e exclusões podem tomar lugar apenas em um extremo, chamado de "topo" da lista. Essa estrutura é semelhante em sua operação a uma pilha de pratos em um sistema de mola, como descrito na Fig. 8-4(*a*). Observe que novos pratos são inseridos apenas no topo da pilha e pratos podem ser retirados apenas do topo da pilha.

Algoritmo 8.1: O nome de um vendedor é lido e a lista de seus clientes é impressa.

Passo 1. Ler XXX.

Passo 2. Encontrar K tal que VENDEDOR[K] = XXX [Use busca binária]

Passo 3. Faça PTR := START[K]. [Inicializa apontador PTR]

Passo 4. Repita enquanto PTR ≠ NULL.

(a) Imprimir CLIENTE[PTR].

(b) Faça PTR := NEXT[PTR]. [Atualiza PTR.]

[Fim do ciclo]

Passo 5. Saída.

Figura 8-3

(b) **Fila:** Uma *fila* (*queue*, em inglês), também chamada de sistema "primeiro a entrar é o primeiro a sair" (FIFO, sigla inglês para *first-in-first-out*), é uma lista linear na qual deleções somente podem ocorrer em um extremo da lista, à "frente", e inserções somente podem acontecer no outro extremo, no "final". A estrutura opera de maneira muito semelhante a uma fila de pessoas esperando por um ônibus, como retratado na Fig. 8-4(*b*). Ou seja, a primeira pessoa na fila é a primeira a entrar no ônibus, e uma nova pessoa vai para o fim da fila.

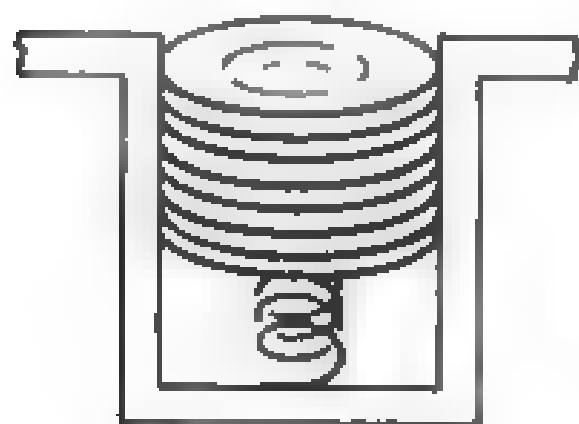
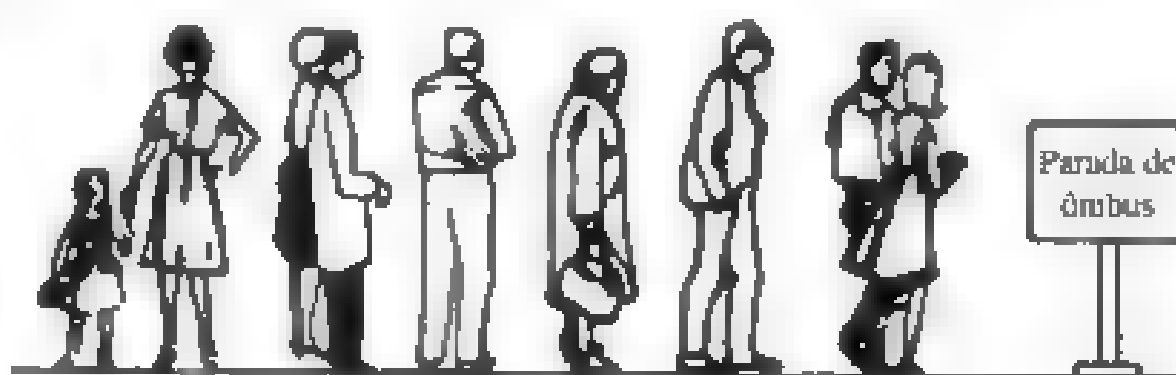
(c) **Fila de prioridade:** Seja S um conjunto no qual novos elementos podem ser periodicamente inseridos, mas tal que o atual maior elemento (aquele com a "maior prioridade") é sempre deletado. Então S é chamado de *fila de prioridade*. As regras "mulheres e crianças primeiro" e "os mais velhos primeiro" são exemplos de filas de prioridade. Pilhas e filas comuns são tipos especiais de filas de prioridade. Especificamente, o elemento com a maior prioridade em uma pilha é o último elemento inserido, mas aquele com a maior prioridade em uma fila é o primeiro inserido.

(*a*) Pilha de pratos (*b*) Fila de pessoas esperando por um ônibus

Figura 8-4

8.2 GRAFOS E MULTIGRAFOS

Um grafo G consiste em duas coisas:

(i) Um conjunto $V = V(G)$ cujos elementos são chamados de *vértices*, *pontos* ou *nós* de G.

(ii) Um conjunto $E = E(G)$ de pares não ordenados de vértices distintos chamados de *arestas* de G.

Denotamos tal grafo por $G(V, E)$ quando queremos enfatizar as duas partes de G.

Os vértices u e v são ditos *adjacentes* ou *vizinhos* se existe uma aresta $e = \{u, v\}$. Em tal caso, u e v são chamados de *extremos* de e, e dizemos que *e conecta u e v*. Além disso, a aresta e é dita *incidente* sobre cada um de seus extremos u e v. Os grafos são representados por diagramas no plano de maneira natural. Especificamente, cada vértice v em V é representado por um ponto (ou um pequeno círculo), e cada aresta $e = \{v_1, v_2\}$ é representada por uma curva que conecta seus extremos v_1 e v_2. Por exemplo, a Fig. 8-5(a) corresponde ao grafo $G(V, E)$, onde:

(i) V consiste nos vértices A, B, C e D.

(ii) E consiste nas arestas $e_1 = \{A, B\}$, $e_2 = \{B, C\}$, $e_3 = \{C, D\}$, $e_4 = \{A, C\}$ e $e_5 = \{B, D\}$.

De fato, em geral denotamos um grafo desenhando seu diagrama em vez de listar explicitamente seus vértices e arestas.

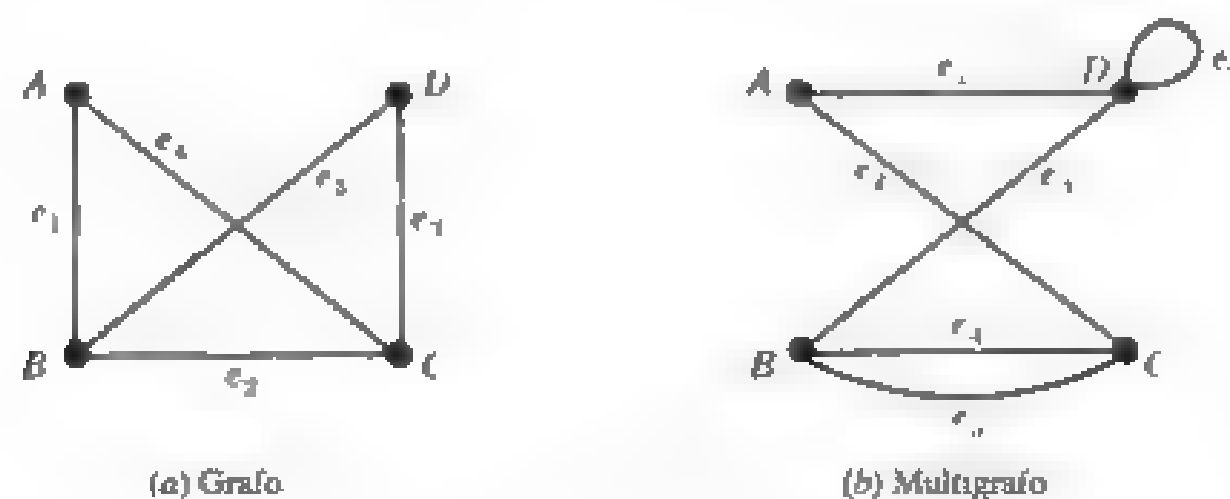



Figura 8-5

Multigrafos

Considere o diagrama na Fig. 8-5(b): e_4 e e_5 são chamados de *arestas múltiplas*, uma vez que elas conectam os mesmos extremos, e a aresta e_6 é dita um laço (*loop*), pois seus extremos são o mesmo vértice. Tal diagrama é chamado de *multigrafo*; a definição formal de grafo não permite múltiplas arestas nem laços.

Observação: Alguns textos usam o termo *grafo* para incluir multigrafos e empregam a expressão *grafo simples* para se referir a um grafo sem múltiplas arestas e laços.

Grau de um vértice

O *grau* de um vértice v em um grafo G, denotado por deg(v), é igual ao número de arestas em G que contêm v, isto é, que são incidentes sobre v. Como cada aresta é contada duas vezes na contagem dos graus dos vértices de G, temos o seguinte resultado simples, mas importante.

Teorema 8.1: A soma dos graus dos vértices de um grafo G é igual ao dobro do número de arestas em G.

Considere, por exemplo, o grafo na Fig. 8-5(a). Temos

$$\deg(A) = 2, \deg(B) = 3, \deg(C) = 3, \deg(D) = 2.$$

A soma dos graus é 10, o que, como esperado, é o dobro do número de arestas. Um vértice é dito *par* ou *ímpar* dependendo se seu grau é um número par ou ímpar. Assim, A e D são vértices pares, enquanto B e C são vértices ímpares.

O Teorema 8.1 também vale para multigrafos, onde um laço é contado duas vezes através do grau de seu extremo. Por exemplo, na Fig. 8-5(b) temos deg(D) = 4, pois a aresta e_6 é contada duas vezes, logo, D é um vértice par.

Um vértice de grau zero é chamado de vértice *isolado*.

Grafos finitos, grafo trivial

Um multigrafo é dito *finito* se tiver um número finito de vértices e uma quantia finita de arestas. Observe que um grafo com um número finito de vértices deve automaticamente ter uma quantia finita de arestas e, portanto, deve ser finito. O grafo finito com um vértice e nenhuma aresta, isto é, um único ponto, é chamado de *grafo trivial*. A menos que seja dito o contrário, os multigrafos neste livro são finitos.

8.3 SUBGRAFOS, GRAFOS ISOMORFOS E HOMEOMORFOS

Esta seção discute relações importantes entre grafos.

Subgrafos

Considere um grafo $G = G(V, E)$. Um grafo $H = H(V', E')$ é dito um subgrafo de G se os vértices e arestas de H estão contidos nos vértices e arestas de G, ou seja, $V' \subseteq V$ e $E' \subseteq E$. Especificamente.

(i) Um subgrafo $H(V', E')$ de $G(V, E)$ é chamado de subgrafo *induzido* por seus vértices V', se seu conjunto de arestas E' contém todas as arestas em G cujos extremos pertencem a vértices em H.

(ii) Se v é um vértice em G, então $G - v$ é o subgrafo de G, obtido ao deletar v de G, bem como todas as arestas em G que contêm v.

(iii) Se e é uma aresta em G, então $G - e$ é o subgrafo de G, obtido ao deletar a aresta e de G.

Grafos isomorfos

Os grafos $G(V, E)$ e $G^*(V^*, E^*)$ são ditos isomorfos se existe uma correspondência bijetora $f: V \to V^*$ tal que $\{u, v\}$ é uma aresta de G se, e somente se, $\{f(u), f(v)\}$ é uma aresta de G^*. Normalmente, não distinguimos entre grafos isomorfos (apesar de seus diagramas poderem "parecer diferentes"). A Fig. 8-6 mostra dez grafos representados como letras. Observamos que A e R são grafos isomorfos, assim como F e T, K e X e M, S, V e Z.

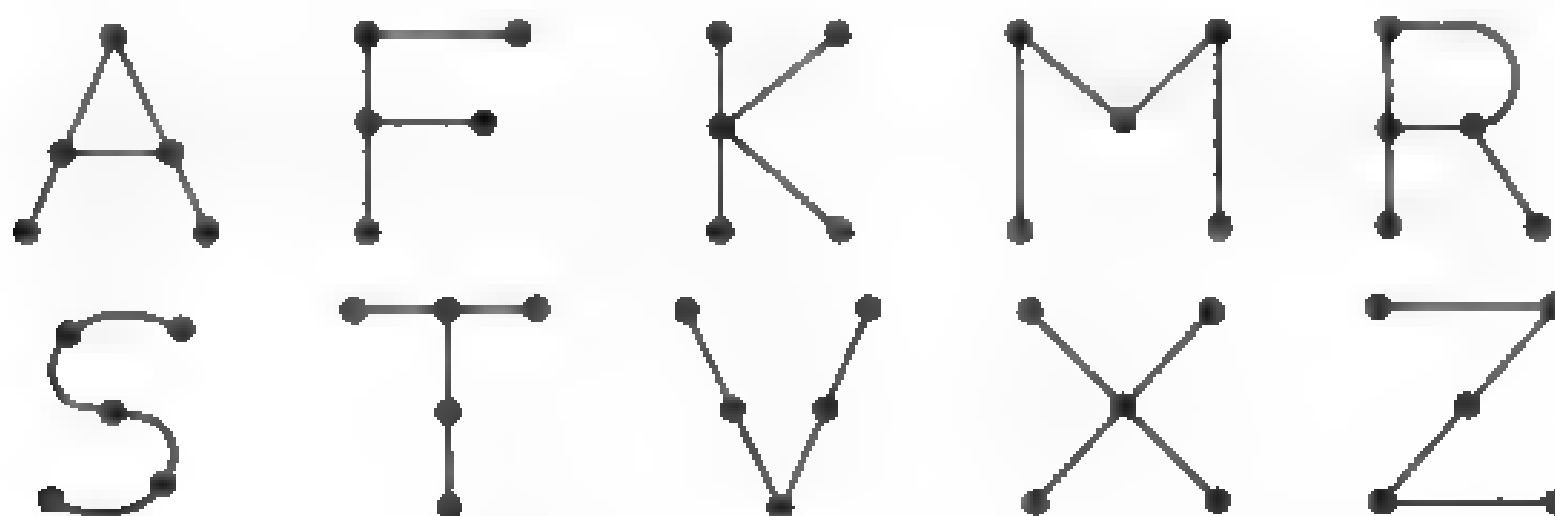



Figura 8-6

Grafos homeomorfos

Dado qualquer grafo G, podemos obter um novo grafo, dividindo uma aresta de G com vértices adicionais. Dois grafos G e G^* são ditos *homeomorfos* se puderem ser obtidos a partir do mesmo grafo, ou de grafos isomorfos, por esse método. Os grafos (a) e (b) na Fig. 8-7 não são isomorfos, mas são homeomorfos, pois ambos podem ser obtidos a partir do grafo (c) pelo acréscimo de vértices adequados.

Figura 8-7

8.4 CAMINHOS, CONECTIVIDADE

Um *caminho* em um multigrafo G consiste em uma sequência alternada de vértices e arestas da forma

$$v_0, e_1, v_1, e_2, v_2, \ldots, e_{n-1}, v_{n-1}, e_n, v_n$$

onde cada aresta e_i contém os vértices v_{i-1} e v_i (que aparecem nos lados de e_i na sequência). O número n de arestas é chamado de *comprimento* do caminho. Quando não há ambiguidade, denotamos um caminho por sua sequência de vértices $(v_0, v_1, \ldots, v_n)$. O caminho é dito *fechado* se $v_0 = v_n$. Caso contrário, dizemos que o caminho é de v_0 a v_n, ou *entre* v_0 e v_n, ou que *conecta* v_0 com v_n.

Um *caminho simples* é um caminho no qual todos os vértices são distintos. (Um caminho no qual todas as arestas são distintas chama-se *trilha*.) Um *ciclo* é um caminho fechado de comprimento 3, ou maior, no qual todos os vértices são distintos, exceto $v_0 = v_n$. Um ciclo de comprimento k é chamado de *k-ciclo*.

Exemplo 8.1 Considere o grafo G na Fig. 8-8(*a*). Considere as sequências a seguir:

$$\alpha = (P_4, P_1, P_2, P_5, P_1, P_2, P_3, P_6),\ \beta = (P_4, P_1, P_5, P_2, P_6),$$
$$\gamma = (P_4, P_1, P_5, P_2, P_3, P_5, P_6),\ \delta = (P_4, P_1, P_5, P_3, P_6).$$

A sequência α é um caminho de P_4 a P_6, mas não é uma trilha, pois a aresta $\{P_1, P_2\}$ é usada duas vezes. A sequência β não é um caminho, uma vez que não há aresta $\{P_2, P_6\}$. A sequência γ é uma trilha, pois nenhuma aresta é usada duas vezes; mas ela não é um caminho simples, visto que o vértice P_5 é usado duas vezes. A sequência δ é um caminho simples de P_4 a P_6, mas não é o caminho mais curto (em relação a comprimento) de P_4 a P_6. O caminho mais curto de P_4 a P_6 é (P_4, P_5, P_6), que tem comprimento 2.

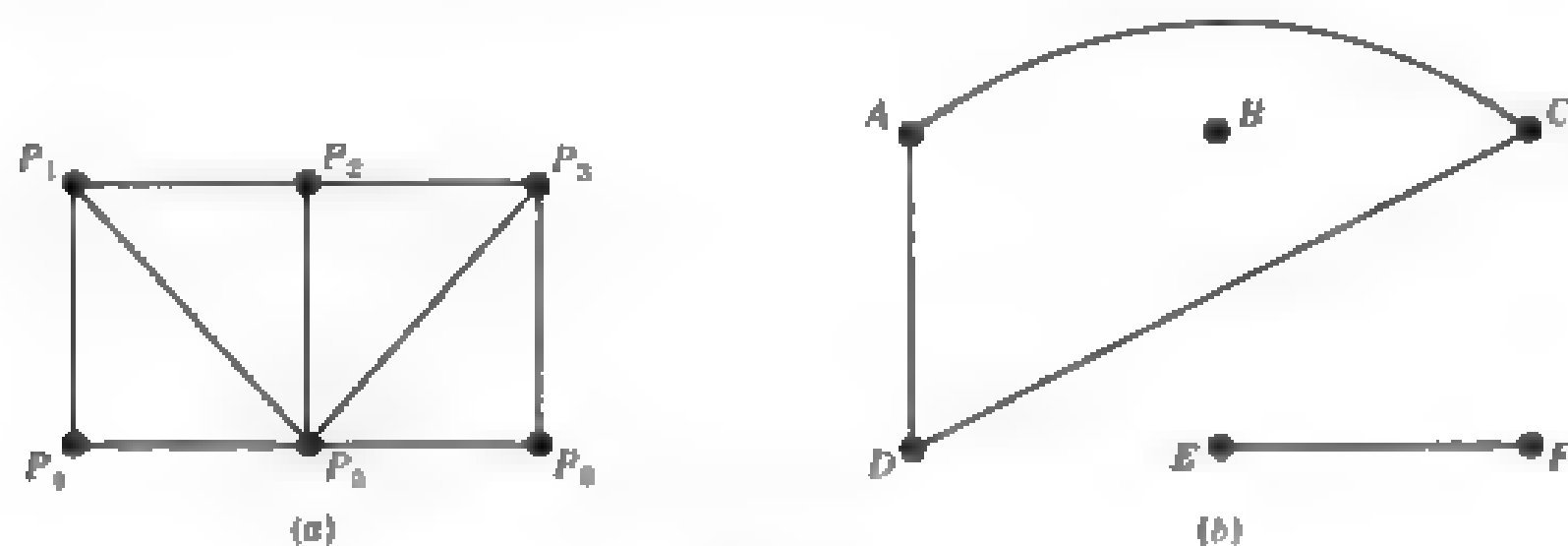



Figura 8-8

Eliminando arestas desnecessárias, não é difícil perceber que qualquer caminho de um vértice u a um vértice v pode ser substituído por um caminho simples de u a v. Estabelecemos esse resultado formalmente.

Teorema 8.2: Existe um caminho de um vértice u a um vértice v se, e somente se, existe um caminho simples de u a v.

Conectividade, componentes conexas

Um grafo G é *conexo* se existe um caminho entre dois quaisquer de seus vértices. O grafo na Fig. 8-8(a) é conexo, mas o grafo na Fig. 8-8(b) não é, pois, por exemplo, não há caminho algum entre os vértices D e E.

Suponha que G é um grafo. Um subgrafo conexo H de G é dito uma componente conexa de G se H não está contido em qualquer subgrafo conexo maior de G. É intuitivamente claro que qualquer grafo G pode ser particionado em suas componentes conexas. Por exemplo, o grafo G na Fig. 8-8(b) tem três componentes conexas, os subgrafos induzidos pelos conjuntos de vértices $\{A, C, D\}$, $\{E, F\}$ e $\{B\}$.

O vértice B na Fig. 8-8(b) é chamado de *vértice isolado*, uma vez que B não pertence a qualquer aresta ou, em outras palavras, $\deg(B) = 0$. Portanto, como observado, B por si só forma uma componente conexa do grafo.

Observação: Formalmente falando, assumir que qualquer vértice u é conexo a si mesmo, a relação "u é conexo a v" é uma relação de equivalência sobre o conjunto de vértices de um grafo G, e as classes de equivalência dessa relação formam as componentes conexas de G.

Distância e diâmetro

Considere um grafo conexo G. A *distância* entre os vértices u e v em G, denotada por $d(u, v)$, é o comprimento do caminho mais curto entre u e v. O *diâmetro* de G, denotado por $\text{diam}(G)$, é a distância máxima entre dois pontos quaisquer de G. Por exemplo, na Fig. 8-9(a), $d(A, F) = 2$ e $\text{diam}(G) = 3$, enquanto na Fig. 8-9(b), $d(A, F) = 3$ e $\text{diam}(G) = 4$.

Pontos de corte e pontes

Seja G um grafo conexo. Um vértice v em G é chamado de *ponto de corte* se $G - v$ é desconexo. (Lembre que $G - v$ é o grafo obtido a partir de G deletando v e todas as arestas contendo v.) Uma aresta e de G é chamada de *ponte* se $G - e$ é desconexo. (Lembre que $G - e$ é o grafo obtido a partir de G deletando a aresta e.) Na Fig. 8-9(a) o vértice D é um ponto de corte e não há pontes. Na Fig. 8-9(b) a aresta $= \{D, F\}$ é uma ponte. (Seus pontos extremos D e F são necessariamente pontos de corte.)

Figura 8-9

8.5 GRAFOS ATRAVESSÁVEIS E EULERIANOS, PONTES DE KÖNIGSBERG

A cidade do século XVIII, no leste da Prússia, de Königsberg, incluía duas ilhas e sete pontes, como mostrado na Fig. 8-10(a). Começando em qualquer ponto e terminando em qualquer ponto, uma pessoa pode caminhar pela cidade atravessando todas as sete pontes, sem passar por qualquer ponte duas vezes? O povo de Königsberg escreveu para o célebre matemático suíço L. Euler sobre essa questão. Euler provou em 1736 que tal jornada é impossível. Ele substituiu as ilhas e os dois lados do rio por pontos, e as pontes por curvas, obtendo a Fig. 8-10(b).

Observe que a Fig. 8-10(b) é um multigrafo. Um multigrafo é dito *atravessável* se ele "puder ser desenhado sem interrupções no trajeto e sem repetir quaisquer arestas", ou seja, se existe um caminho que inclui todos os vértices e usa cada aresta exatamente uma vez. Tal caminho deve ser uma trilha (uma vez que nenhuma aresta é

utilizada duas vezes) e é chamado de *trilha atravessável*. Evidentemente, um multigrafo atravessável deve ser finito e conexo.

(*a*) Königsberg em 1736 (*b*) Representação gráfica de Euler

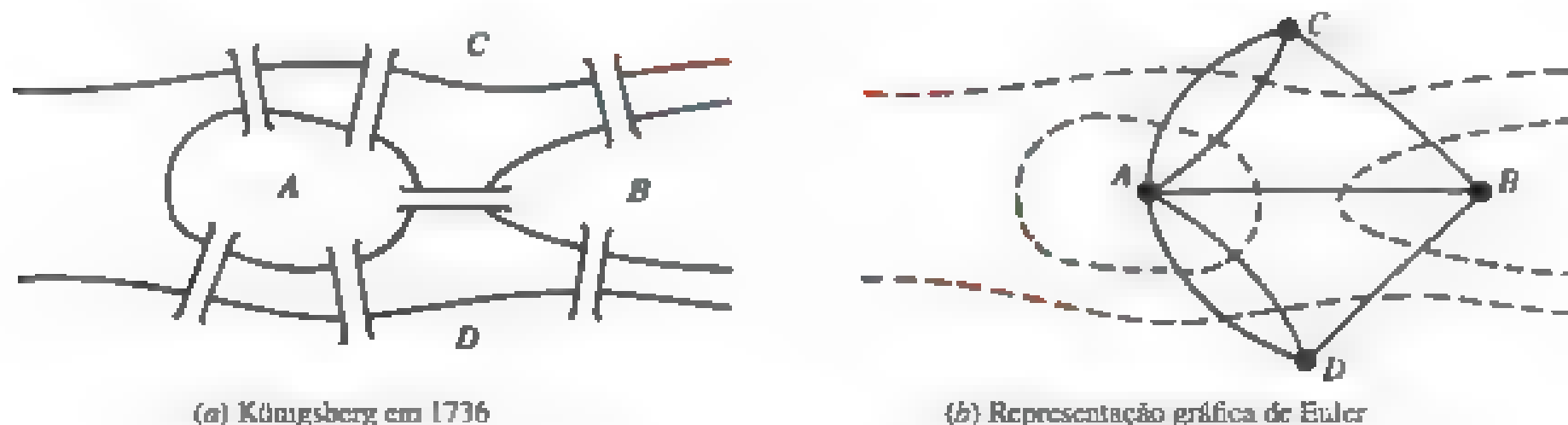



Figura 8-10

Mostramos agora como Euler provou que o multigrafo na Fig. 8-10(*b*) não é atravessável e, portanto, que a caminhada em Königsberg é impossível. Lembre que um vértice é par ou ímpar se seu grau é um número par ou ímpar. Suponha que um multigrafo é atravessável e que uma trilha atravessável não começa ou termina em um vértice *P*. Afirmamos que *P* é um vértice par. Afinal, sempre que a trilha atravessável entra em *P*, por uma aresta, deve haver uma aresta não usada anteriormente, pela qual a trilha deve sair de *P*. Assim, as arestas da trilha incidentes sobre *P* devem aparecer aos pares e, logo, *P* é um vértice par. Portanto, se um vértice *Q* é ímpar, a trilha atravessável deve começar ou terminar em *Q*. Consequentemente, um multigrafo com mais de dois vértices ímpares não pode ser atravessável. Observe que o multigrafo correspondente ao problema da ponte de Königsberg tem quatro vértices ímpares. Logo, não se pode caminhar por Königsberg, de modo que cada ponte seja atravessada exatamente uma vez.

Na verdade, Euler demonstrou a recíproca da afirmação acima, que está contida no teorema a seguir e em seu corolário. (O teorema é demonstrado no Problema 8.9.) Um grafo *G* é chamado de *euleriano* se existe uma trilha atravessável fechada, conhecida como trilha *euleriana*.

Teorema 8.3 (Euler): Um grafo conexo finito é euleriano se, e somente se, cada vértice tem grau par.

Corolário 8.4: Qualquer grafo conexo finito com dois vértices ímpares é atravessável. Uma trilha atravessável pode começar em qualquer um dos vértices ímpares e terminar no outro vértice ímpar.

Grafos hamiltonianos

A discussão acima sobre grafos eulerianos enfatizou arestas para a viagem; aqui nos concentramos em vértices para visitar. Um *circuito hamiltoniano* em um grafo *G*, nomeado em homenagem ao matemático irlandês do século XIX, William Hamilton (1803–1865), é um caminho fechado que visita cada vértice de *G* exatamente uma vez. (Tal caminho fechado deve ser um ciclo.) Se *G* admite um circuito hamiltoniano, então *G* é dito um *grafo hamiltoniano*. Observe que um circuito euleriano percorre cada aresta exatamente uma vez, mas pode repetir vértices, enquanto um circuito hamiltoniano visita cada vértice exatamente uma vez, mas pode repetir arestas. A Fig. 8-11 dá um exemplo de um grafo que é hamiltoniano, mas não euleriano, e vice-versa.

(*a*) Hamiltoniano e não euleriano

(*b*) Euleriano e não hamiltoniano

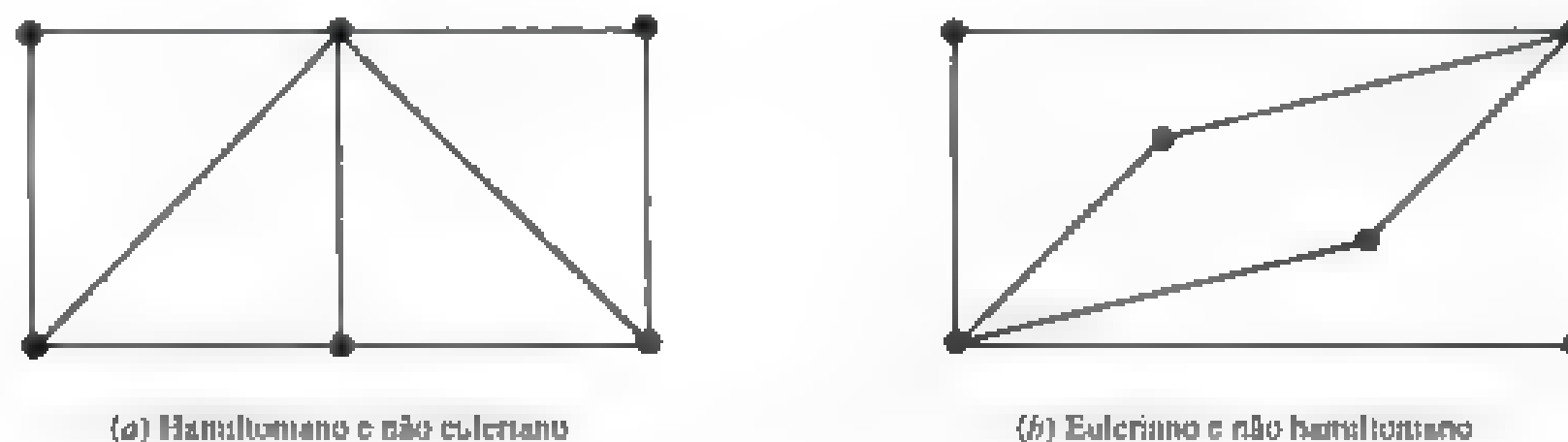



Figura 8-11

Apesar de ser claro que apenas grafos conexos podem ser hamiltonianos, não há critério algum para nos dizer se um grafo é hamiltoniano, como existe para grafos eulerianos. Temos a seguinte condição suficiente que é devida a G. A. Dirac.

Teorema 8.5: Seja G um grafo conexo com n vértices. Então G é hamiltoniano, se $n \geq 3$ e $n \leq \deg(v)$ para cada vértice v em G.

8.6 GRAFOS ROTULADOS E PONDERADOS

G é chamado de *grafo rotulado* se suas arestas e/ou vértices são assinalados a dados de algum tipo. Especificamente, G é chamado de *grafo ponderado* se cada aresta e de G é assinalada com um número não negativo $w(e)$, conhecido como o *peso* ou *comprimento* de v. A Fig. 8-12 mostra um grafo ponderado, onde o peso de cada aresta é dado da maneira óbvia. O *peso* (ou *comprimento*) de um caminho em tal grafo ponderado é definido como a soma dos pesos das arestas no caminho. Um problema importante na teoria dos grafos é encontrar o caminho *mais curto*, ou seja, um caminho de peso (comprimento) mínimo entre dois vértices quaisquer. O comprimento de um caminho mais curto entre P e Q na Fig. 8-12 é 14, tal caminho é

$$(P, A_1, A_2, A_5, A_3, A_6, Q)$$

O leitor pode tentar encontrar outro caminho mais curto.

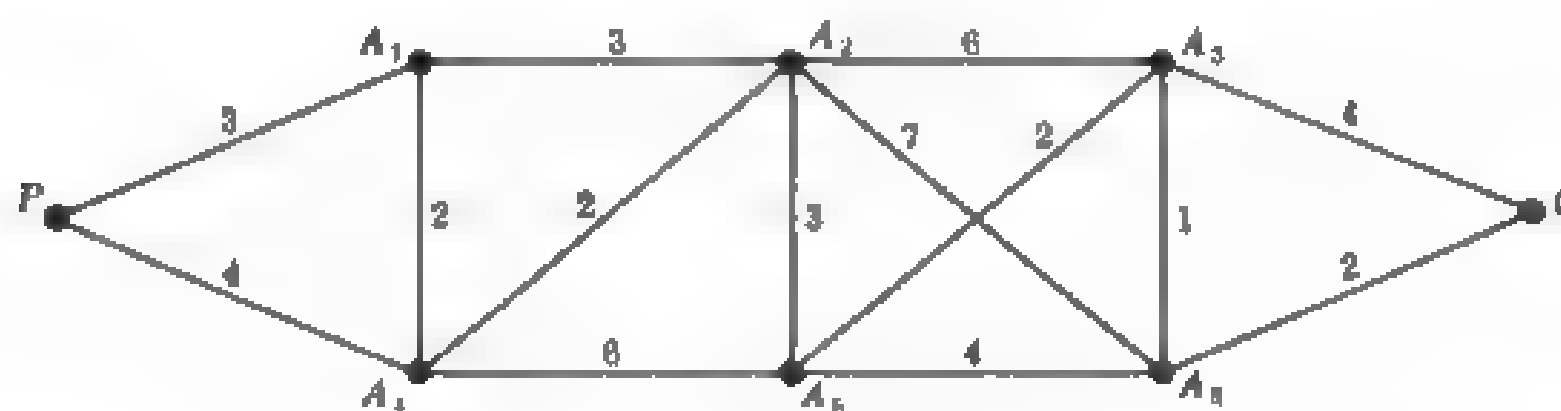



Figura 8-12

8.7 GRAFOS COMPLETOS, REGULARES E BIPARTIDOS

Há muitos tipos diferentes de grafos. Esta seção considera três deles: completos, regulares e bipartidos.

Grafos completos

Um grafo G é dito *completo* se todo vértice em G é conectado a todos os demais vértices de G. Assim, um grafo completo G deve ser conexo. O grafo completo com n vértices é denotado por K_n. A Fig. 8-13 mostra os grafos K_1 a K_6.

Grafos regulares

Um grafo G é *regular* de *grau k* ou *k-regular* se todo vértice tem grau k. Em outras palavras, um grafo é regular se todo vértice tem o mesmo grau.

Os grafos regulares conexos de graus 0, 1 ou 2 são facilmente descritos. O grafo 0-regular conexo é o grafo trivial com um vértice e nenhuma aresta. O grafo 1-regular conexo é o grafo com dois vértices e uma aresta conectando-os. O grafo 2-regular conexo com n vértices é o grafo que consiste em um único n-ciclo. Ver Fig. 8-14.

Os grafos 3-regulares devem ter um número par de vértices, uma vez que a soma dos graus dos vértices é um número par (Teorema 8.1). A Fig. 8-15 mostra dois grafos 3-regulares conexos com seis vértices. No caso geral, grafos regulares podem ser muito complicados. Por exemplo, há dezenove grafos 3-regulares com dez vértices. Observamos que o grafo completo com n vértices K_n é regular de grau $n-1$.

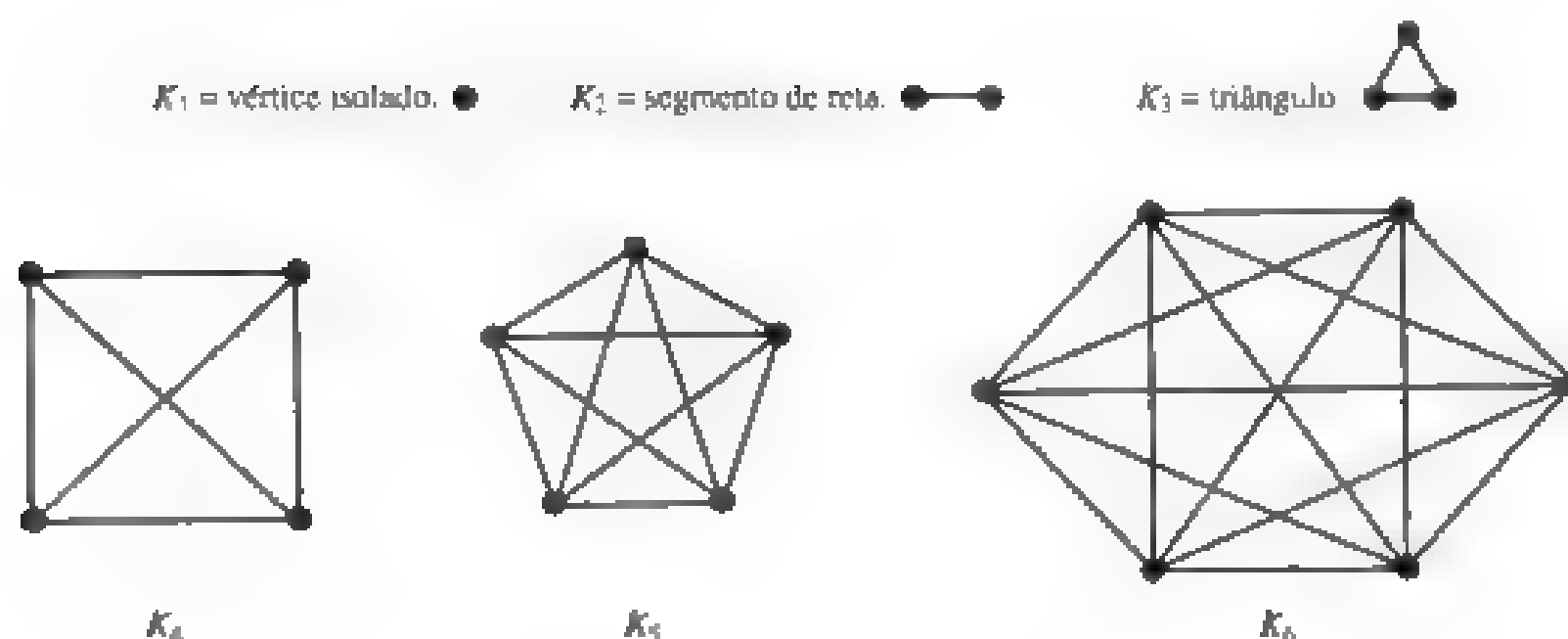



Figura 8-13

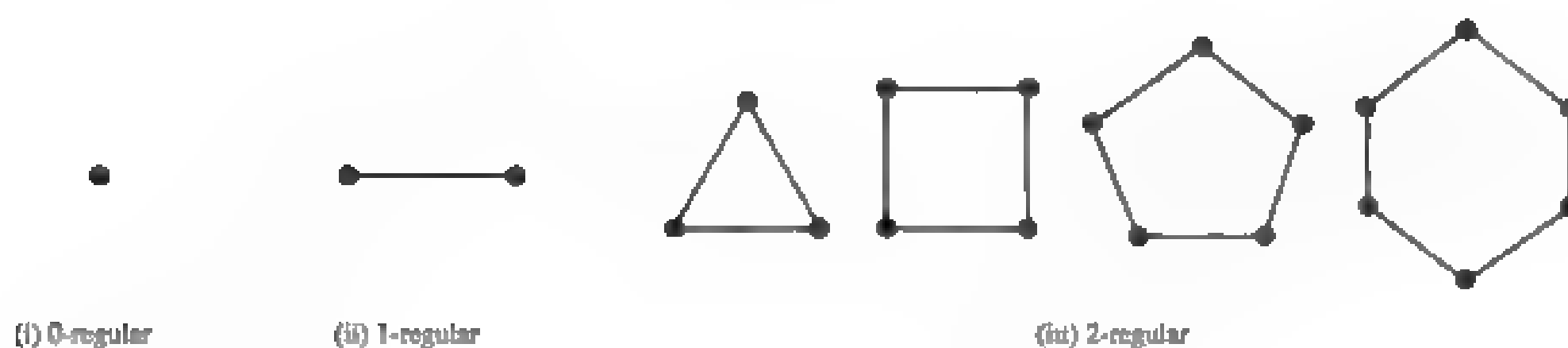



Figura 8-14

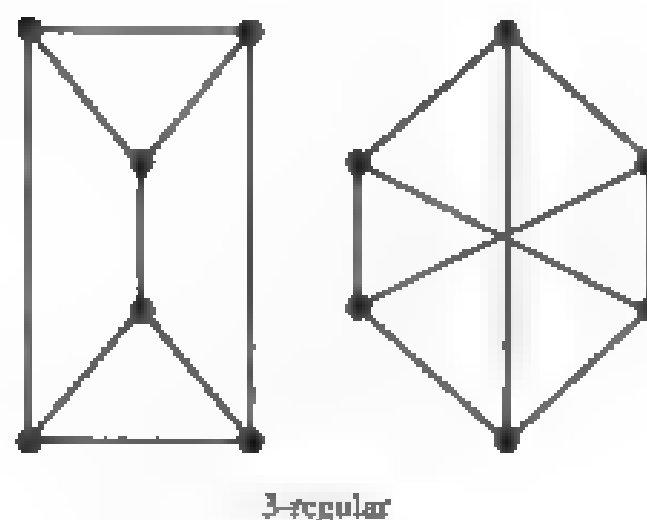



Figura 8-15

Grafos bipartidos

Um grafo G é dito *bipartido* se seus vértices V podem ser particionados em dois subconjuntos M e N tais que cada aresta de G conecta um vértice de M a um vértice de N. Por grafo bipartido completo, queremos dizer que cada vértice de M é conectado a cada vértice de N; este grafo é denotado por $K_{m,n}$, onde m é o número de vértices em M e n é o número de vértices em N, e, para padronização, assumimos que $m \leq n$. A Fig. 8-16 mostra os grafos $K_{2,3}$, $K_{3,3}$ e $K_{2,4}$. Claramente o grafo $K_{m,n}$ tem mn arestas.

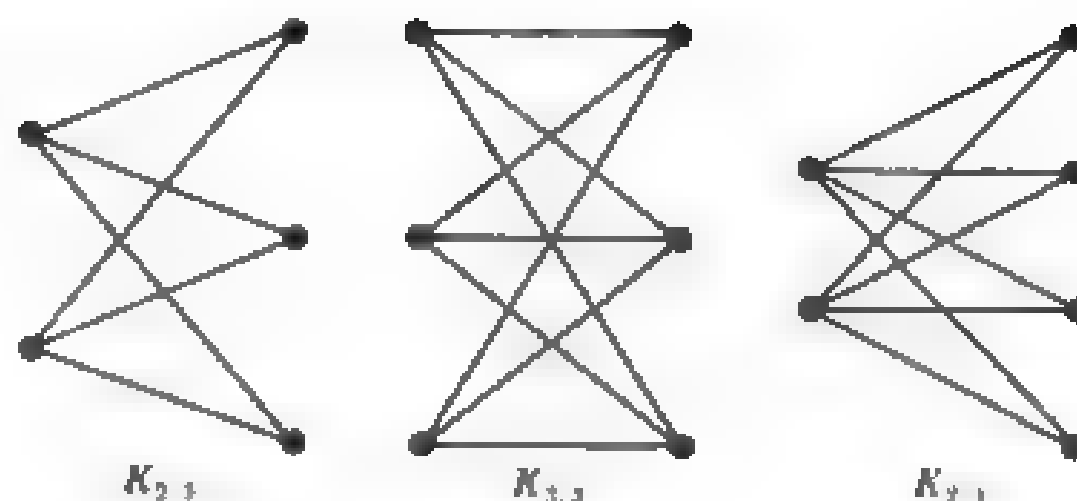



Figura 8-16

8.8 GRAFOS EM ÁRVORE

Um grafo T é chamado de *árvore* se for conexo e sem ciclos. Exemplos de árvores são mostrados na Fig. 8-17. Uma *floresta* G é um grafo sem ciclos; logo, as componentes conexas de uma floresta G são árvores. Um grafo sem ciclos é dito *acíclico*. A árvore consistindo em um único vértice sem arestas é chamada de *árvore degenerada*.

Considere uma árvore T. Claramente, há apenas um caminho simples entre dois vértices de T; caso contrário, os dois caminhos formariam um ciclo. Além disso:

(a) Suponha que não existe aresta $\{u, v\}$ em T e que acrescentemos a aresta $e = \{u, v\}$ a T. Então o caminho simples de u a v em T e e formam um ciclo; logo, T não é mais uma árvore.

(b) Por outro lado, suponha que existe uma aresta $e = \{u, v\}$ em T e então deletamos e de T. Portanto, T não é mais conexo (pois não pode haver um caminho de u a v); assim, T não é mais uma árvore.

O teorema a seguir (demonstrado no Problema 8.14) se aplica quando nossos grafos são finitos.

Teorema 8.6: Seja G um grafo com $n > 1$ vértices. Então o que se segue são equivalências:

(i) G é uma árvore.

(ii) G é acíclico e tem $n - 1$ arestas.

(iii) G é conexo e tem $n - 1$ arestas.

Esse teorema também nos diz que uma árvore finita T com n vértices deve ter $n - 1$ arestas. Por exemplo, a árvore na Fig. 8-17(a) tem 9 vértices e 8 arestas, e a árvore na Fig. 8-17(b) tem 13 vértices e 12 arestas.

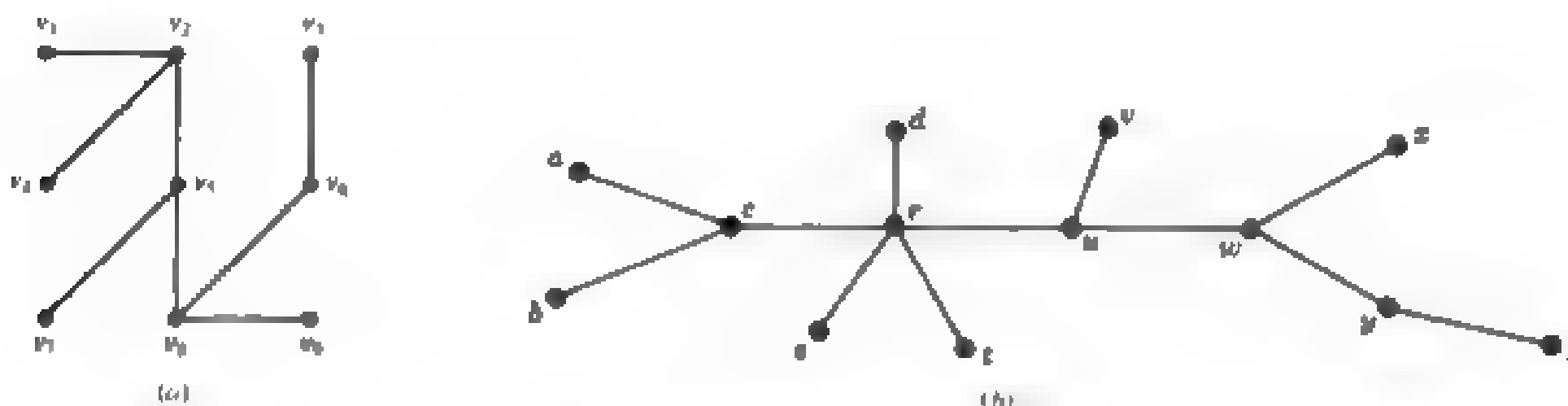



Figura 8-17

Árvores geradoras

Um subgrafo T de um grafo conexo G é dito uma *árvore geradora* de G se T for uma árvore e incluir todos os vértices de G. A Fig. 8-18 mostra um grafo conexo G e árvores geradoras T_1, T_2 e T_3 de G.

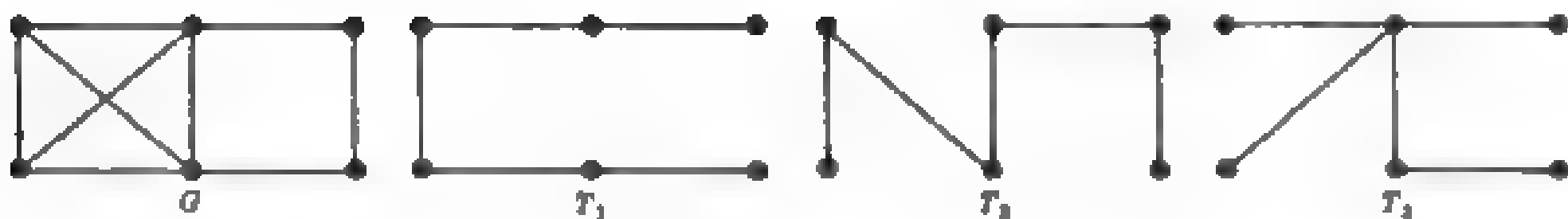



Figura 8-18

Árvores geradoras mínimas

Suponha que G é um grafo ponderado conexo. Ou seja, cada aresta de G é assinalada a um número não negativo chamado de *peso* da aresta. Então, qualquer árvore geradora T de G é assinalada a um peso total obtido pela adição dos pesos das arestas em T. Uma *árvore geradora mínima* de G é uma árvore geradora cujo peso total é tão pequeno quanto possível.

Os algoritmos 8.2 e 8.3, que aparecem na Fig. 8-19, permitem encontrar uma árvore geradora mínima T de um grafo ponderado conexo G, onde G tem n vértices. (Caso em que T deve ter $n - 1$ vértices.)

Algoritmo 8.2: A entrada é um grafo ponderado conexo G com n vértices.

Passo 1. Arrange as arestas de G na ordem de pesos decrescentes.

Passo 2. Procedendo sequencialmente, delete cada aresta que não desconecta o grafo até restarem $n - 1$ arestas.

Passo 3. Saída.

Algoritmo 8.3 (Kruskal): A entrada é um grafo ponderado conexo G com n vértices.

Passo 1. Arrange as arestas de G em ordem crescente de pesos.

Passo 2. Comece apenas com os vértices de G e, procedendo sequencialmente, acrescente cada aresta que não resulte em um ciclo até $n - 1$ arestas serem acrescentadas.

Passo 3. Saída.

Figura 8-19

O peso de uma árvore geradora mínima é único, mas ela em si não é. Diferentes árvores geradoras mínimas podem ocorrer quando duas ou mais arestas têm o mesmo peso. Em tal caso, o arranjo das arestas no Passo 1 do Algoritmo 8.2 ou 8.3 não é único e, logo, pode resultar em diferentes árvores geradoras mínimas, como ilustrado no exemplo a seguir.

Exemplo 8.2 Encontre uma árvore geradora mínima do grafo ponderado Q na Fig. 8-20(a). Observe que Q tem seis vértices e, assim, uma árvore geradora mínima terá cinco arestas.

(a) Aqui aplicamos o Algoritmo 8.2.

Primeiro, ordenamos as arestas por pesos decrescentes e, então, sucessivamente deletamos arestas sem desconectar Q, até restarem cinco arestas. Isso conduz aos dados a seguir:

Arestas	BC	AF	AC	BE	CE	BF	AE	DF	BD
Peso	8	7	7	7	6	5	4	4	3
Deletar?	Sim	Sim	Sim	Não	Não	Sim			

Assim, a árvore geradora mínima de Q obtida contém as arestas

$$BE, CE, AE, DF, BD$$

A árvore geradora tem peso 24 e é mostrada na Fig. 8-20(b)

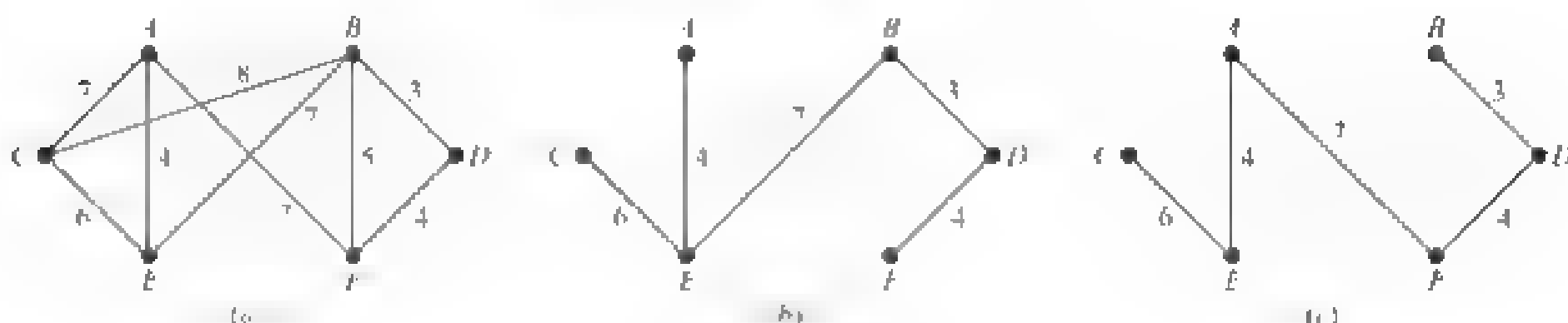



Figura 8-20

(b) Aqui aplicamos o Algoritmo 8.3.

Primeiro, ordenamos as arestas por pesos crescentes e, então, sucessivamente adicionamos arestas sem formar quaisquer ciclos, até cinco arestas serem incluídas. Isso nos leva aos seguintes dados:

Arestas	BD	AE	DF	BF	CE	AC	AF	BE	BC
Peso	3	4	4	5	6	7	7	7	8
Adiciona?	Sim	Sim	Sim	Não	Sim	Não	Sim		

Assim, a árvore geradora mínima de Q obtida contém as arestas

$$BD, AE, DF, CE, AF$$

A árvore geradora aparece na Fig. 8-20(c). Observe que essa árvore geradora não é a mesma obtida, ao usar o Algoritmo 8.2. Como esperado, ela também tem peso 24.

Observação: Os algoritmos acima são facilmente executados quando o grafo G é relativamente pequeno, como na Fig. 8-20(a). Suponha que G tem dúzias de vértices e centenas de arestas que, digamos, são dados por uma lista de pares de vértices. Então, mesmo decidir se G é conexo não é óbvio; isso pode requerer algum tipo de algoritmo de busca em profundidade (DFS, na sigla em inglês para *depth-first search*) ou busca em largura (BFS, *breadth-first search*). Seções adiante e o próximo capítulo discutem maneiras de representar grafos G em memória, bem como vários algoritmos.

8.9 GRAFOS PLANARES

Um grafo ou multigrafo que pode ser desenhado no plano, de modo que suas arestas não se cruzem é dito *planar*. Apesar de o grafo completo com quatro vértices K_4 ser geralmente representado com arestas que se cruzam, como na Fig. 8-21(a), ele pode também ser desenhado com arestas que não se cruzam, como na Fig. 8-21(b); logo, K_4 é planar. Gráficos em árvore formam uma classe importante de grafos planares. Esta seção introduz o leitor a esses importantes grafos.

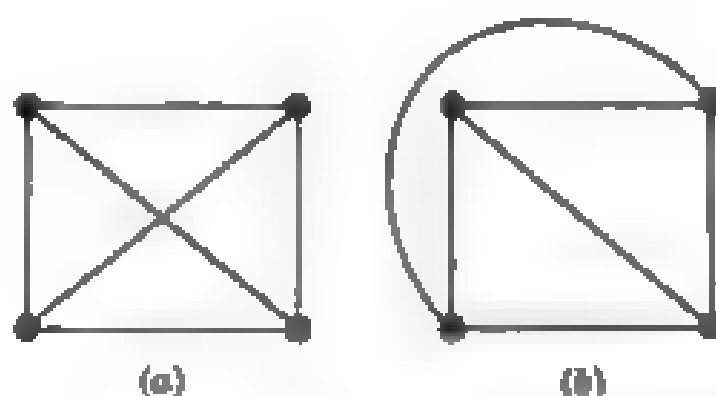



Figura 8-21

Mapas, regiões

Uma representação plana específica de um multigrafo planar é chamada de *mapa*. Dizemos que o mapa é *conexo* se o multigrafo subjacente for conexo. Um dado mapa divide o plano em várias regiões. Por exemplo, o mapa na Fig. 8-22 com seis vértices e nove arestas divide o plano em cinco regiões. Observe que quatro das regiões são limitadas, mas a quinta, fora do diagrama, é ilimitada. Logo, não há perda de generalidade ao contarmos o número de regiões, se assumirmos que nosso mapa está contido em algum grande retângulo em vez do plano inteiro.

Observe que a fronteira de cada região de um mapa consiste em arestas. Às vezes as arestas formam um ciclo, mas às vezes não. Por exemplo, na Fig. 8-22 as fronteiras de todas as regiões são ciclos, exceto por r_3. Contudo, se nos movemos no sentido anti-horário em torno de r_3, começando, digamos, no vértice C, obtemos o caminho fechado

$$(C, D, E, F, E, C)$$

onde a aresta $\{E, F\}$ ocorre duas vezes. Por *grau* de uma região r, denotado por $\deg(r)$, queremos dizer o comprimento do ciclo ou caminho fechado que circunda r. Observamos que cada aresta estabelece fronteira com duas regiões ou está contido em uma região e ocorre duas vezes em qualquer trajeto ao longo da fronteira da região. Assim, temos um teorema para regiões que é análogo ao Teorema 8.1 para vértices.

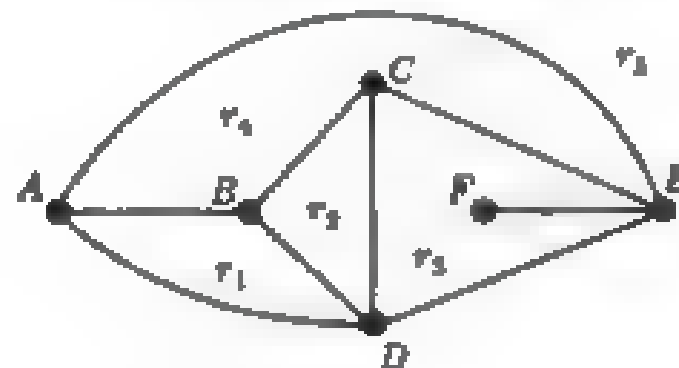



Figura 8-22

Teorema 8.7: A soma dos graus das regiões de um mapa é igual ao dobro do número de arestas.

Os graus das regiões da Fig. 8-22 são:

$$\deg(r_1) = 3,\ \deg(r_2) = 3,\ \deg(r_3) = 5,\ \deg(r_4) = 4,\ \deg(r_5) = 3$$

A soma dos graus é 18, que, como esperado, é duas vezes o número de arestas.

Por conveniência notacional, devemos representar os vértices de um mapa com pontos ou pequenos círculos, ou devemos assumir que quaisquer interseções de retas ou curvas no plano são vértices.

Fórmula de Euler

Euler forneceu uma fórmula que relaciona o número V de vértices, o número E de arestas e o número R de regiões para qualquer mapa conexo. Especificamente:

Teorema 8.8 (Euler): $V - E + R = 2$.

(A demonstração do Teorema 8.8 aparece no Problema 8.18.)

Observe que, na Fig. 8-22, $V = 6$, $E = 9$ e $R = 5$, e, como antecipado pela fórmula de Euler,

$$V - E + R = 6 - 9 + 5 = 2$$

Enfatizamos que o grafo subjacente ao mapa deve ser conexo para a fórmula de Euler valer.

Seja G um multigrafo planar conexo com três ou mais vértices, de modo que G não é K_1 nem K_2. Seja M uma representação planar de G. Não é difícil perceber que (1) uma região de M pode ter grau 1 apenas se sua fronteira é um laço, e (2) uma região de M pode ter grau 2 somente se sua fronteira consiste em duas arestas múltiplas. Consequentemente, se G é um grafo, não um multigrafo, então toda região de M deve ter grau 3 ou maior. Esse comentário, junto com a fórmula de Euler, é usado para provar o seguinte resultado sobre grafos planares.

Teorema 8.9: Seja G um grafo planar conexo com p vértices e q arestas, onde $p \geq 3$. Então, $q \leq 3p - 6$.

Observe que o teorema não vale para K_1, onde $p = 1$ e $q = 0$, e não é verdadeiro para K_2, onde $p = 2$ e $q = 1$.

Demonstração: Seja r o número de regiões em uma representação planar de G. Pela fórmula de Euler, $p - q + r = 2$.

A soma dos graus das regiões é $2q$, pelo Teorema 8.7. Mas cada região tem grau 3 ou maior; logo, $2q \geq 3r$. Assim, $r \leq 2q/3$. Substituindo isso na fórmula de Euler, temos

$$2 = p - q + r \leq p - q + \frac{2q}{3} \quad \text{ou} \quad 2 \leq p - \frac{q}{3}$$

Multiplicando a desigualdade por 3, temos $6 \geq 3p - q$, que nos dá nosso resultado.

Estou aqui

Grafos não planares, teorema de Kuratowski

Fornecemos dois exemplos de grafos não planares. Considere primeiro o *grafo de serviços*, ou seja, três casas A_1, A_2 e A_3 devem ser conectadas a serviços de água, gás e eletricidade, B_1, B_2 e B_3, como na Fig. 8-23(a). Observe que esse é o grafo $K_{3,3}$, que tem $p = 6$ vértices e $q = 9$ arestas. Suponha que o grafo é planar. Pela fórmula de Euler, uma representação planar tem $r = 5$ regiões. Observe que nenhum trio de vértices é conectado um ao outro; logo, o grau de cada região deve ser 4 ou maior e, assim, a soma dos graus das regiões deve ser 20 ou maior. Pelo Teorema 8.7, o grafo deve ter 10 ou mais arestas. Isso contradiz o fato de que o grafo tem 9 arestas. Logo, o grafo de serviços $K_{3,3}$ é não planar.

V - E + R = 2
6 - 9 + R = 2
R = 5

Considere a seguir o *grafo estrela* na Fig. 8-23(b). Esse é o grafo completo K_5 sobre $p = 5$ vértices e tem $q = 10$ arestas. Se o grafo é planar, então pelo Teorema 8.9,

$$10 = q \leq 3p - 6 = 15 - 6 = 9$$

V - E + R = 2
5 - 10 + R = 2
R = 7 mas neste caso tem 11 regiões.

o que é impossível. Portanto, K_5 é não planar.

Por muitos anos, matemáticos tentaram caracterizar grafos planares e não planares. O problema foi finalmente resolvido pelo matemático polonês K. Kuratowski. A demonstração desse resultado, dada abaixo, está além do escopo deste livro.

(a) $K_{3,3}$

(b) K_5

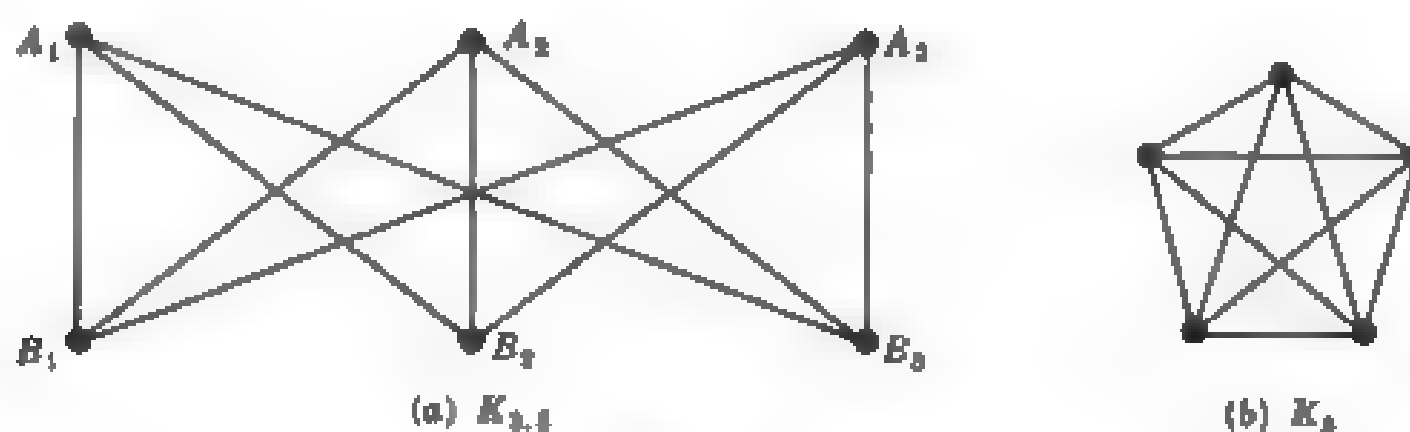



Figura 8-23

Teorema 8.10 (Kuratowski). Um grafo é não planar se, e somente se, ele contém um subgrafo homeomorfo a $K_{3,3}$ ou K_5.

8.10 COLORAÇÃO DE GRAFOS

Considere um grafo G. Uma *coloração de vértice*, ou simplesmente uma *coloração* de G, é uma atribuição de cores aos vértices de G tal que vértices adjacentes têm cores diferentes. Dizemos que G é n-colorível se existe uma coloração de G que usa n cores. O número mínimo de cores necessárias para pintar G é chamado de *número cromático* de G e é denotado por $\chi(G)$.

A Fig. 8-24 fornece um algoritmo de Welch e Powell para a coloração de um grafo G. Enfatizamos que esse algoritmo nem sempre conduz a uma coloração mínima de G.

Algoritmo 8.4 (Welch-Powell): A entrada é um grafo G.

Passo 1. Ordene os vértices de G de acordo com graus decrescentes.

Passo 2. Assinale a primeira cor C_1 ao primeiro vértice e, então, em ordem sequencial, assinale C_1 a cada vértice que não é adjacente ao vértice anterior que foi assinalado por C_1.

Passo 3. Repita o Passo 2 com uma segunda cor C_2 e a subsequência de vértices não coloridos.

Passo 4. Repita o Passo 3 com uma terceira cor C_3 e, então, uma quarta cor C_4, e assim por diante, até todos os vértices estarem coloridos.

Passo 5. Saída.

Figura 8-24

Exemplo 8.3

(*a*) Considere o grafo G na Fig. 8-25. Usamos o Algoritmo 8.4 de Welch-Powell para obter uma coloração de G. Ordenando os vértices por graus decrescentes, temos a seguinte sequência:

$$A_5, A_3, A_7, A_1, A_2, A_4, A_6, A_8$$

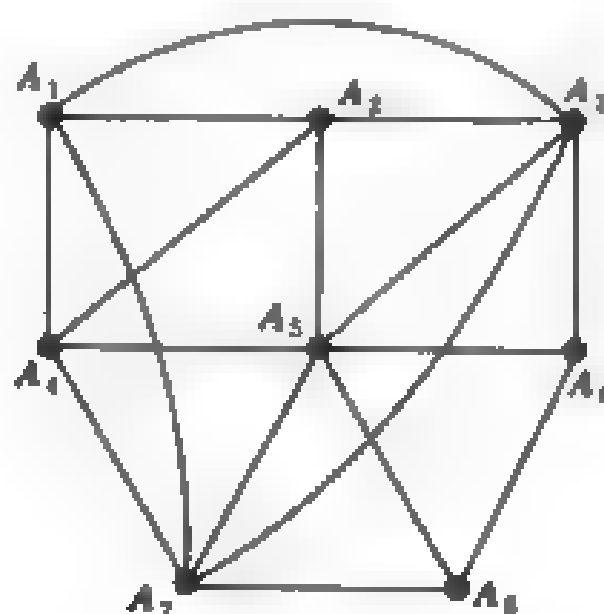



Figura 8-25

A primeira cor é assinalada aos vértices A_5 e A_1. A segunda cor é assinalada aos vértices A_3, A_4 e A_8. A terceira cor é assinalada aos vértices A_7, A_2 e A_6. Todos os vértices foram assinalados a uma cor e, assim, G é 3-colorível. Note que G não é 2-colorível, pois os vértices A_1, A_2 e A_3, que são conectados um ao outro, devem ser correspondidos a cores diferentes. Consequentemente, $\chi(G) = 3$.

(b) Considere o grafo completo K_n com n vértices. Uma vez que cada vértice é adjacente aos demais, K_n exige n cores em qualquer coloração. Assim, $\chi(K_n) = n$.

Não há maneira simples para realmente determinar se um grafo qualquer é n-colorível. Porém, o teorema a seguir (provado no Problema 8.19) fornece uma caracterização simples de grafos 2-colorizáveis.

Teorema 8.11: As seguintes afirmações são equivalentes para um grafo G:

(i) G é 2-colorível.

(ii) G é bipartido.

(iii) Todo ciclo de G tem comprimento par.

Não há limite sobre o número de cores que podem ser necessárias para a coloração de um mapa arbitrário, pois, por exemplo, o grafo completo K_n demanda n cores. No entanto, se nos restringirmos a grafos planares, independentemente do número de vértices, cinco cores bastam. De modo mais específico, no Problema 8.20 demonstramos:

Teorema 8.12: Qualquer grafo planar é 5-colorível.

Na verdade, desde a década de 1850, matemáticos têm conjecturado que grafos planares são 4-colorizáveis, uma vez que todo grafo planar conhecido é 4-colorível. Kenneth Appel e Wolfgang Haken finalmente provaram que essa conjectura é verdadeira em 1976. Ou seja:

Teorema das Quatro Cores (Appel e Haken): Qualquer grafo planar é 4-colorível.

Discutimos esse teorema na próxima subseção.

Mapas duais e o teorema das quatro cores

Considere um mapa M, digamos, o mapa M na Fig. 8-26(a). Em outras palavras, M é uma representação planar de um multigrafo planar. Duas regiões de M são ditas *adjacentes* se tiverem uma aresta em comum. Logo, as regiões r_2 e r_5 na Fig. 8-26(a) são adjacentes, mas as regiões r_3 e r_5 não são. Por uma *coloração* de M, queremos dizer uma designação de uma cor para cada região de M, tal que regiões adjacentes têm cores diferentes. Um mapa M é n-*colorível* se existe uma coloração de M que emprega n cores. Assim, o mapa M na Fig. 8-26(a) é 3-colorível, pois as regiões podem ser assinaladas às seguintes cores:

r_1 vermelho, r_2 branco, r_3 vermelho, r_4 branco, r_5 vermelho, r_6 azul

Observe a semelhança entre essa discussão sobre coloração de mapas e a anterior sobre coloração de grafos. De fato, usando o conceito de mapa dual definido abaixo, a coloração de um mapa pode ser mostrada como sendo equivalente à coloração de vértices de um grafo planar.

Considere um mapa M. Em cada região de M escolhemos um ponto e, se duas regiões têm uma aresta em comum, então conectamos os pontos correspondentes com uma curva através da aresta em comum. Essas curvas podem ser desenhadas, de modo que elas não se cruzem. Logo, obtemos um novo mapa M^*, chamado de *dual* de M, tal que cada vértice de M^* corresponde a exatamente uma região de M. A Fig. 8-26(b) mostra o dual do mapa na Fig. 8-26(a). Pode-se provar que cada região de M^* contém exatamente um vértice de M e que cada aresta de M^* intersecta exatamente uma aresta de M e vice-versa. Portanto, M é o dual do mapa M^*.

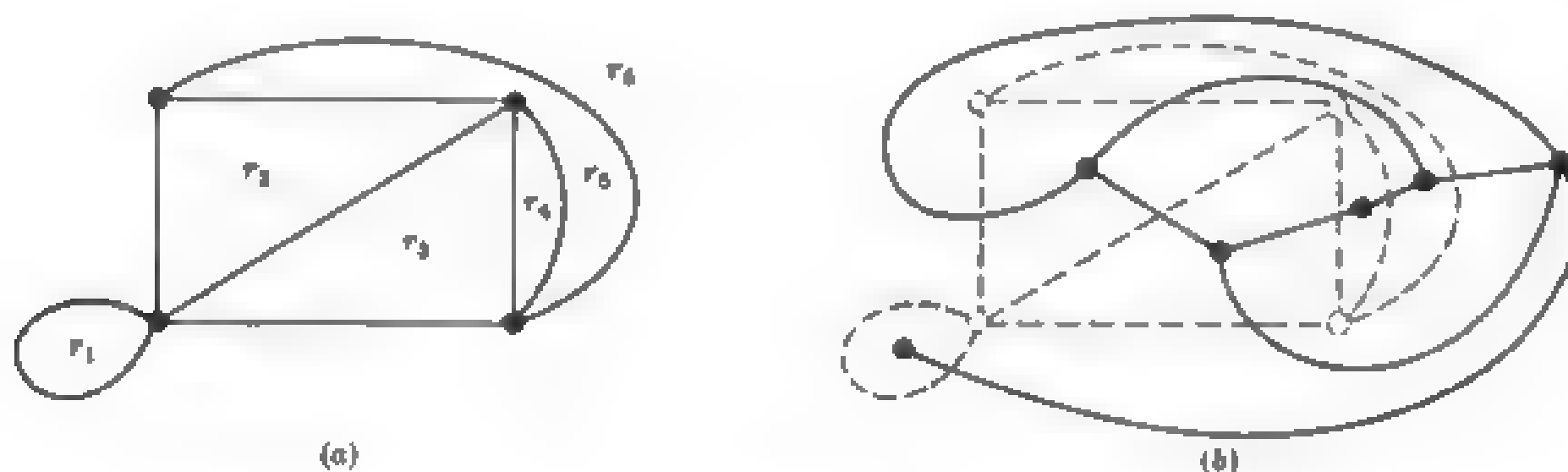



Figura 8-26

Note que qualquer coloração das regiões de um mapa corresponde a uma coloração dos vértices do mapa dual M^*. Assim, M é n-colorível se, e somente se, o grafo planar do mapa dual M^* é n-colorível (nos vértices). Logo, o teorema acima pode ser reescrito como se segue:

Teorema das Quatro Cores (Appel e Haken): Se as regiões de qualquer mapa M são colorizadas, de modo que regiões adjacentes têm cores diferentes, então não mais do que quatro cores são necessárias.

A demonstração do teorema anterior usa computadores como um passo essencial. Appel e Haken, em especial, primeiro mostraram que se o teorema das quatro cores for falso, então deve haver um contraexemplo entre aproximadamente 2000 tipos diferentes de grafos planares. Depois, usando o computador, demonstraram que nenhum desses tipos de grafos se mostra como um contraexemplo. O exame de cada tipo diferente de grafo parece estar além da capacidade do ser humano, sem a ajuda de um computador. Portanto, a prova, diferente da maioria das demonstrações em matemática,† é dependente da tecnologia; ou seja, ela depende do desenvolvimento de computadores de alta velocidade.

8.11 REPRESENTANDO GRAFOS NA MEMÓRIA DO COMPUTADOR

Existem duas maneiras usuais para manter um grafo G na memória de um computador. Uma delas, chamada de *representação sequencial* de G, é através de sua matriz de adjacência A. A outra, conhecida como *representação ligada* ou *estrutura de adjacência* de G, emprega listas ligadas de vizinhos. Matrizes são geralmente utilizadas quando o grafo G é denso, e listas ligadas são usualmente empregadas quando G é esparso. (Um grafo G com m vértices e n arestas é dito *denso* quando $m = O(n^2)$ e esparso quando $m = O(n)$ ou mesmo quando $O(n \log n)$.)

Independentemente da maneira como se mantém um grafo G na memória, em geral ele é inserido no computador por sua definição formal, ou seja, como uma coleção de vértices e uma coleção de pares de vértices (arestas).

Matriz de adjacência

Suponha que G é um grafo com m vértices e que os vértices tenham sido ordenados, digamos, $v_1, v_2, \ldots, v_m$. Então a *matriz de adjacência* $A = [a_{ij}]$ do grafo G é a matriz $m \times m$ definida por

$$a_{ij} = \begin{cases} 1 & \text{se } v_i \text{ é adjacente a } v_j \\ 0 & \text{caso contrário} \end{cases}$$

A Fig. 8-27(b) contém a matriz de adjacência do grafo G na Fig. 8-27(a), onde os vértices são ordenados A, B, C, D, E. Observe que cada aresta $\{v_i, v_j\}$ de G é representada duas vezes, por $a_{ij} = 1$ e $a_{ji} = 1$. Logo, neste caso, a matriz de adjacência é simétrica.

A matriz de adjacência A de um grafo G depende da ordenação dos vértices de G, isto é, uma ordem diferente dos vértices conduz a uma matriz de adjacência diferente. Porém, duas matrizes de adjacência do mesmo grafo estão fortemente relacionadas entre si, de modo que uma pode ser obtida a partir da outra simplesmente permutando linhas e colunas. Por outro lado, a matriz de adjacência não depende da ordem na qual as arestas (pares de vértices) são inseridas no computador.

Há variações da representação acima. Se G é um multigrafo, então normalmente denotamos a_{ij} pelo número de arestas $\{v_i, v_j\}$. Além disso, se G é um grafo ponderado, então podemos fazer com que a_{ij} denote o peso da aresta $\{v_i, v_j\}$.

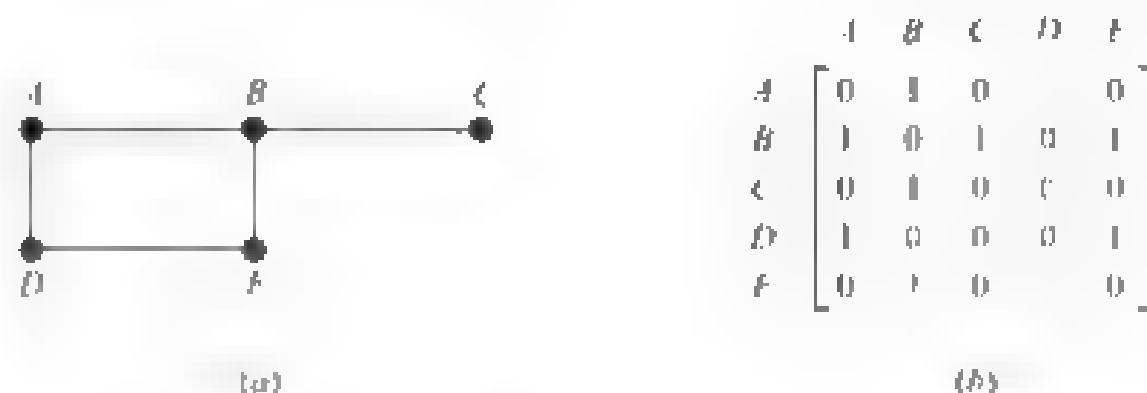



Figura 8-27

† N. de T. Os autores se referem às demonstrações existentes na literatura especializada e não a todas as possíveis demonstrações de todos os possíveis teoremas.

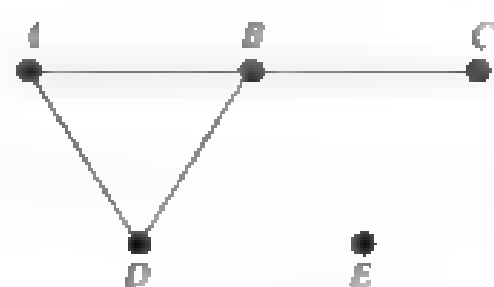
Representação ligada de um grafo G

Seja G um grafo com m vértices. A representação de G na memória através de sua matriz de adjacência A tem uma série de desvantagens consideráveis. Em primeiro lugar, pode ser muito difícil inserir ou deletar vértices de G. O motivo é que o tamanho de A pode mudar e os vértices podem precisar ser reordenados. Logo, podem ocorrer muitas, muitas mudanças na matriz A. Além disso, suponha que o número de arestas é $O(m)$ ou $O(m \log m)$, ou seja, suponha que G é esparso. Então a matriz A contém muitos zeros; logo, um excessivo espaço de memória será desperdiçado. Consequentemente, quando G é esparso, em geral ele é representado na memória por algum tipo de *representação ligada*, também conhecida como *estrutura de adjacência*, a qual é descrita abaixo por meio de um exemplo.

Considere o grafo G na Fig. 8-28(a). Observe que G pode ser equivalentemente definido pela tabela da Fig 8-28(b), a qual mostra cada vértice de G seguido por sua *lista de adjacência*, isto é, sua lista de vértices adjacentes (*vizinhos*). Aqui o símbolo $\varnothing$ denota uma lista vazia. Essa tabela pode ser apresentada também na forma compacta

$$G = [A{:}B, D;\ B{:}A, C, D;\ C{:}B;\ D{:}A, B;\ E{:}\varnothing]$$

onde o símbolo ":" separa um vértice de sua lista de vizinhos, e o símbolo ";" separa as diferentes listas.

Observação: Note que cada aresta de um grafo G é representada duas vezes em uma estrutura de adjacência; ou seja, qualquer aresta, digamos, $\{A, B\}$, é representada por B na lista de adjacência de A e, também, por A na lista de adjacência de B. O grafo G na Fig. 8-28(a) tem quatro arestas e, assim, deve haver oito vértices nas listas de adjacência. Por outro lado, cada vértice em uma lista de adjacência corresponde a uma única aresta no grafo G.

(a)

Vértice	Lista de Adjacência
A	B, D
B	A, C, D
C	B
D	A, B
E	$\varnothing$

(b)

Figura 8-28

A *representação ligada* de um grafo G, que mantém G na memória usando suas listas de adjacência, normalmente contém dois arquivos (conjuntos de registros), sendo um chamado de Arquivo Vértice e o outro, de Arquivo Aresta, como se segue.

(a) ***Arquivo Vértice*:** O Arquivo Vértice contém a lista de vértices do grafo G, usualmente mantido por um array ou uma lista ligada. Cada registro do Arquivo Vértice tem a forma

VERTEX	NEXT-V	PTR	

Aqui VERTEX é o nome do vértice, NEXT-V aponta para o próximo na lista dos vértices do Arquivo Vértice quando os vértices são mantidos por uma lista ligada, e **PTR** aponta para o primeiro elemento na lista de adjacência do vértice que aparece no Arquivo Aresta. A área sombreada indica que pode haver outras informações no registro correspondentes ao vértice.

(b) ***Arquivo Aresta*:** O Arquivo Aresta (ou Arquivo *Edge*) contém as arestas do grafo G. Especificamente, o Arquivo Aresta contém todas as listas de adjacência de G, onde cada lista é mantida na memória por uma lista ligada. Cada registro do Arquivo Aresta corresponde a um vértice em uma lista de adjacência e, portanto, a uma aresta de G. O registro geralmente tem a forma

ARESTA	ADJ	NEXT	

Aqui:

(1) ARESTA é o nome da aresta (se tiver alguma).
(2) ADJ aponta para a localização do vértice no Arquivo Vértice.
(3) NEXT aponta para a localização do próximo vértice na lista de adjacência.

Enfatizamos que cada aresta é representada duas vezes no Arquivo Aresta, mas cada registro do arquivo corresponde a uma única aresta. A área sombreada indica que pode haver outras informações no registro correspondente à aresta.

A Fig. 8-29 mostra como o Grafo G da Fig. 8-28(a) pode aparecer na memória. Aqui os vértices de G são mantidos na memória por uma lista ligada, usando a variável START para apontar para o próximo vértice. (Alternativamente, pode-se usar um array linear para a lista de vértices e NEXT-V, assim, seria desnecessário.) Observe que o campo de arestas não é necessário aqui, uma vez que as arestas não têm nomes. A Fig. 8-29 também mostra, com as flechas, a lista de adjacência $[D, C, A]$ do vértice B.

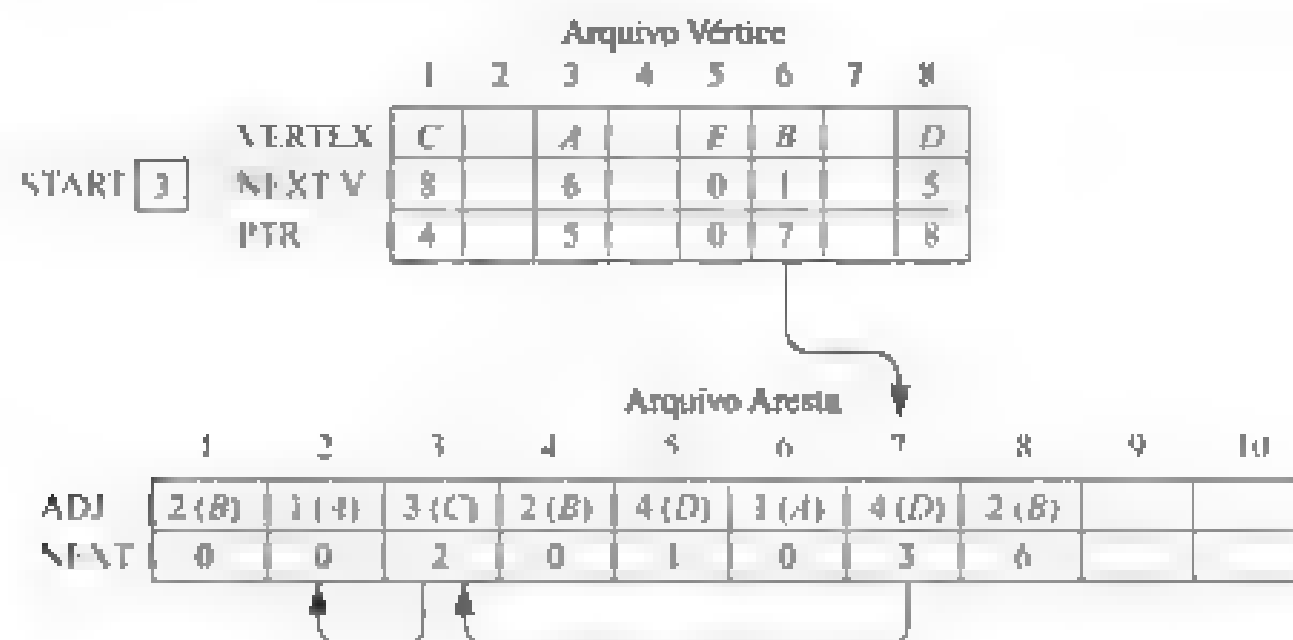



Figura 8-29

8.12 ALGORITMOS DE GRAFOS

Esta seção discute dois algoritmos importantes de grafos que sistematicamente examinam vértices e arestas de um grafo G. Um é chamado de *busca em profundidade* (DFS, na sigla em inglês) e o outro, de *busca em largura* (BFS). Outros algoritmos de grafos são discutidos no próximo capítulo em relação a grafos orientados. Qualquer algoritmo de grafos em particular pode depender da maneira como G é mantido na memória. Aqui assumimos que G é mantido na memória por sua estrutura de adjacência. Nosso grafo teste G com sua estrutura de adjacência aparece na Fig. 8-30, onde assumimos que os vértices são ordenados alfabeticamente.

Vértice	Lista de adjacência
A	B C D
B	A
C	A, K
D	A, K, L
J	L, M
K	C, D, L
L	D, J, K
M	J

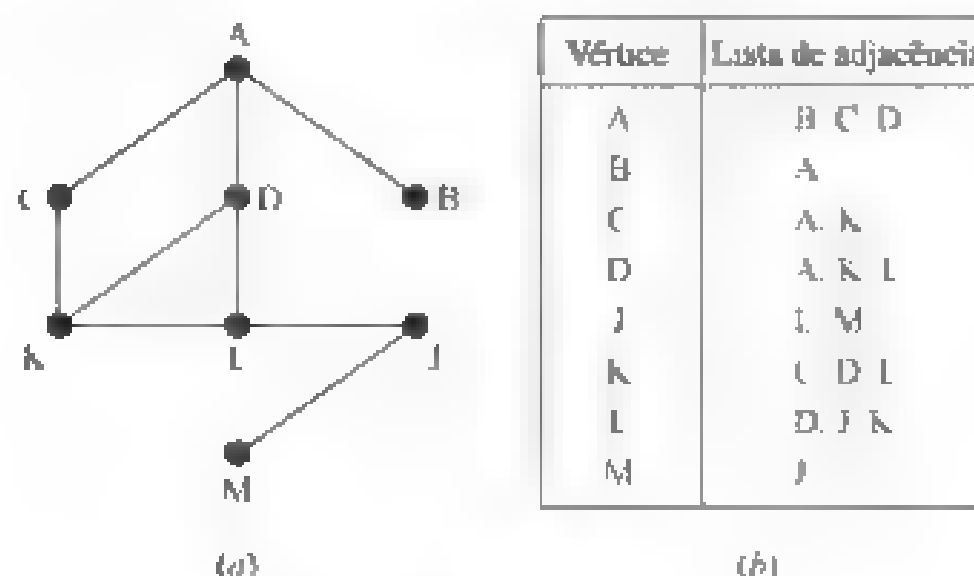



Figura 8-30

Durante a execução de nosso algoritmo, cada vértice (nó) N de G está em um entre três estados, chamados de *status* de N, como se segue:

STATUS = 1: (Estado pronto) O estado inicial do vértice N.

STATUS = 2: (Estado de espera) O vértice N está em uma lista (de espera), aguardando para ser processado.

STATUS = 3: (Estado processado) O vértice N foi processado.

A lista de espera para a busca em profundidade (DFS) é uma PILHA (modificada, a qual escrevemos horizontalmente com o topo da PILHA à esquerda), enquanto a lista de espera para a busca em largura (BFS) é uma FILA.

Busca em profundidade

A ideia geral por trás de uma busca em profundidade começando em um vértice inicial A é como se segue. Primeiro, processamos o vértice inicial A. Em seguida, processamos cada vértice N ao longo de um caminho P que começa em A; ou seja, processamos um vizinho de A, depois outro vizinho de A, e assim por diante. Após chegar a um "beco sem saída", isto é, a um vértice sem vizinho não processado, voltamos pelo caminho P até ser possível continuar por outro caminho P', e assim por diante. A volta é conseguida, usando uma PILHA para manter os vértices iniciais de possíveis caminhos futuros. Precisamos também de um campo STATUS que nos diz o atual estado de qualquer vértice, de modo que nenhum deles seja processado mais de uma vez.

O algoritmo de busca em profundidade (DFS) aparece na Fig. 8-31. O algoritmo processa apenas aqueles vértices que estão conectados com o vértice inicial A, ou seja, a componente conexa que inclui A. Suponha que se deseja processar todos os vértices no grafo G. Então o algoritmo deve ser modificado de forma a começar novamente com outro vértice (que chamamos de B) que ainda esteja no estado pronto (STATUS = 1). Esse vértice B pode ser obtido, percorrendo a lista de vértices.

Observação: A estrutura PILHA no algoritmo acima não é tecnicamente uma pilha, uma vez que, no Passo 5(*b*), permitimos que um vértice J seja deletado e então inserido na frente da pilha. (Apesar de ser o mesmo vértice J, ele geralmente representa uma aresta diferente na estrutura de adjacência.) Se não deletarmos J no Passo 5(*b*), então obtemos uma forma alternativa de DFS.

Algoritmo 8.5 (busca em profundidade): Esse algoritmo executa uma busca em profundidade sobre um grafo G começando com um vértice inicial A.

Passo 1. Inicialize todos os vértices com o estado pronto (STATUS = 1).

Passo 2. Jogue o vértice inicial A na PILHA e mude o estado de A para o de espera (STATUS = 2).

Passo 3. Repita os Passos 4 e 5 até a PILHA estar vazia.

Passo 4. Mova o vértice N do topo da PILHA. Processe N e faça STATUS (N) = 3, o estado processado.

Passo 5. Examine cada vizinho J de N.

(*a*) Se STATUS (J) = 1 (estado pronto), jogue J em PILHA e mude STATUS (N) = 2.

(*b*) Se STATUS (J) = 2 (estado de espera), delete o J anterior da PILHA e jogue o atual J na PILHA.

(*c*) Se STATUS (J) = 3 (estado processado), ignore o vértice J.

[Fim do ciclo do Passo 3.]

Passo 6. Saída.

Figura 8-31

Exemplo 8.4 Suponha que o algoritmo DFS 8.5 da Fig. 8-31 seja aplicado no grafo da Fig. 8-30. Os vértices são processados na seguinte ordem:

$$A, D, L, K, C, J, M, B$$

Especificamente, a Fig. 8-32(*a*) mostra a sequência de vértices sendo processados e a sequência de listas de espera em PILHA. (Note que depois do vértice *A* ser processado, seus vizinhos *B*, *C* e *D* são adicionados à PILHA, em ordem, começando com *B*, depois *C* e finalmente *D*; logo, *D* está no topo da PILHA e *D* é o próximo vértice a ser processado.) Cada vértice, excluindo *A*, vem de uma lista de adjacência e, portanto, corresponde a uma aresta do grafo. Essas arestas formam uma árvore geradora de *G* que é representada na Fig. 8-32(*b*). Os números indicam a ordem que as arestas são adicionadas à árvore geradora, e as linhas tracejadas indicam voltas.

PILHA	Vértice
A	A
D, C, B	D
L, K, C, B	L
K, J, K̸, C, B	K
C, J, C̸, B	C
J, B	J
M, B	M
B	B
∅	

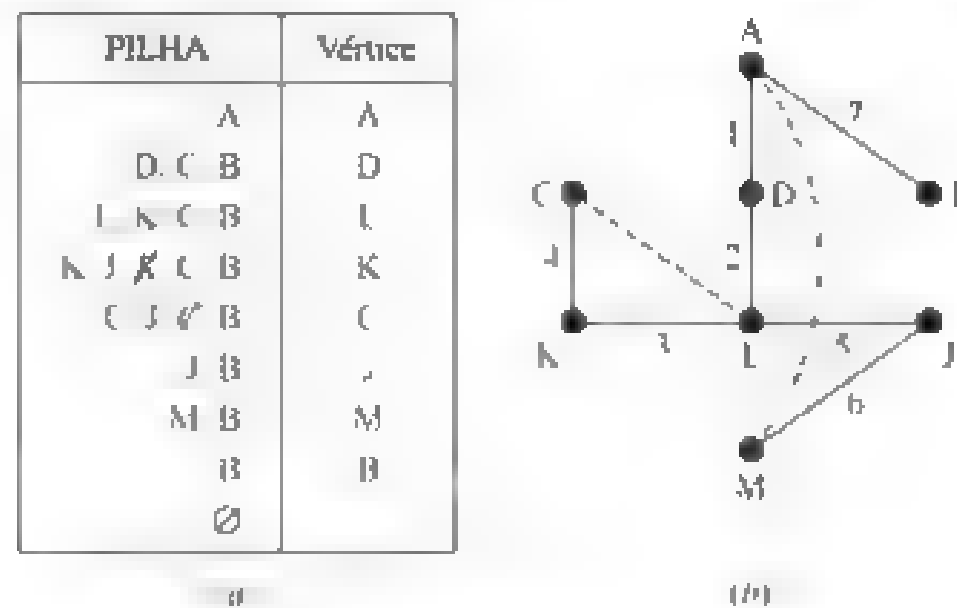



Figura 8-32

Busca em largura

A ideia geral por trás de uma busca em largura começando em um vértice inicial *A* é como se segue. Primeiro, processamos o vértice inicial. Em seguida, processamos todos os vizinhos de *A*. Depois, processamos todos os vizinhos dos vizinhos de *A*, e assim por diante. Naturalmente, precisamos acompanhar os vizinhos de um vértice e garantir que nenhum vértice seja processado duas vezes. Isso se consegue, usando uma FILA para manter os vértices que estão esperando para serem processados, e por um campo STATUS que nos diz o atual estado de um vértice.

O algoritmo de busca em largura (BFS) aparece na Fig. 8-33. Novamente, o algoritmo processa apenas aqueles vértices que estão conectados com o vértice inicial *A*, ou seja, a componente conexa que inclui *A*. Suponha que se deseja processar todos os vértices do grafo *G*. Então o algoritmo deve ser modificado de modo a começar novamen-

Algoritmo 8.6 (busca em largura): Esse algoritmo executa uma busca em largura em um grafo *G* começando com um vértice inicial *A*.

Passo 1. Inicialize todos os vértices com o estado pronto (STATUS = 1).

Passo 2. Coloque o vértice inicial *A* em FILA e mude o estado de *A* para o modo de espera (STATUS = 2).

Passo 3. Repita os Passos 4 e 5 até FILA estar vazia.

Passo 4. Remova o vértice da frente *N* de FILA. Processe *N* e faça STATUS (*N*) = 3, o estado processado.

Passo 5. Examine cada vizinho *J* de *N*.

(*a*) Se STATUS (*J*) = 1 (estado pronto), adicione *J* para o final de FILA e redefina STATUS (*J*) = 2 (estado de espera).

(*b*) Se STATUS (*J*) = 2 (estado de espera) ou STATUS (*J*) = 3 (estado processado), ignore o vértice *J*.

[Fim do ciclo do Passo 3.]

Passo 6. Saída.

Figura 8-33

te com outro vértice (que chamamos de B) que ainda esteja no estado pronto (STATUS = 1). Esse vértice B pode ser obtido por meio da lista de vértices.

Exemplo 8.5 Suponha que o algoritmo de busca em largura (BFS) 8.6 da Fig. 8-33 seja aplicado ao grafo da Fig. 8-30. Os vértices são processados na seguinte ordem

$$A, B, C, D, K, L, J, M$$

Especificamente, a Fig. 8-34(a) mostra a sequência de listas de espera em FILA e a sequência de vértices sendo processados (Observe que depois de o vértice A ser processado, seus vizinhos B, C e D são adicionados à FILA na ordem B, seguido de C e finalmente D; logo, B está na frente da FILA e, assim, B é o próximo vértice a ser processado.) Novamente, cada vértice, excluindo A, vem de uma lista de adjacência e, portanto, corresponde a uma aresta do grafo. Essas arestas formam uma árvore geradora de G que é retratada na Fig. 8-34(b). De novo, os números indicam a ordem em que as arestas são adicionadas à árvore geradora. Observe que essa árvore geradora é diferente daquela da Fig. 8-32(b) que veio de uma busca em profundidade.

FILA	Vértice
A	A
D, C, B	B
D, C	C
D	D
L, K	K
L	L
J	J
M	M
∅	

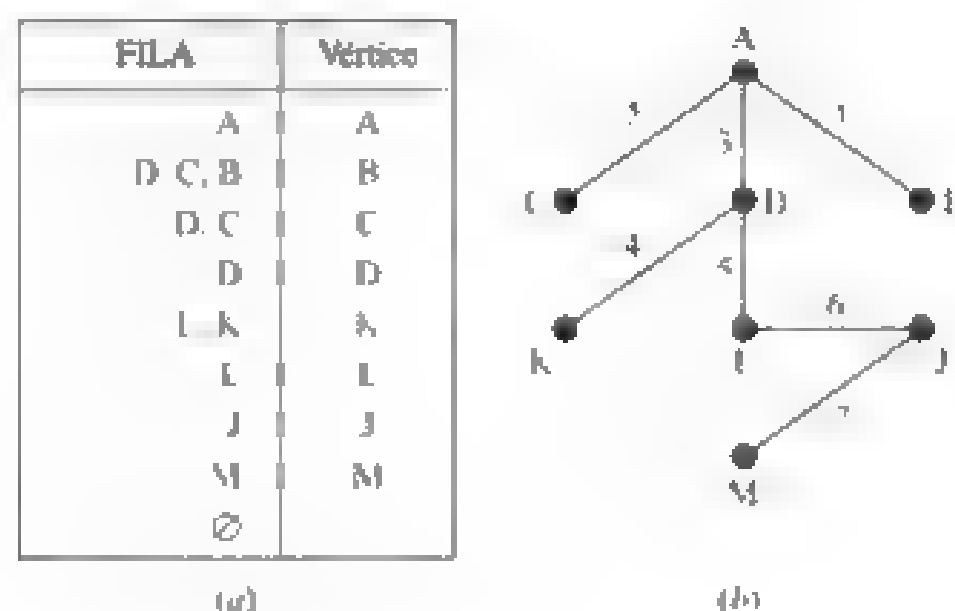



Figura 8-34

8.13 PROBLEMA DO CAIXEIRO VIAJANTE

Seja G um grafo ponderado completo. (Vemos os vértices de G como cidades, e as arestas ponderadas de G como as distâncias entre as cidades.) O problema do "caixeiro viajante" se refere a encontrar um circuito hamiltoniano para G com peso mínimo.

Primeiro observamos o seguinte teorema, demonstrado no Problema 8.33:

Teorema 8.13: O grafo completo K_n com $n \geq 3$ vértices tem $H = (n - 1)!/2$ circuitos hamiltonianos (onde não fazemos distinção entre um circuito e seu reverso).

Considere o grafo ponderado completo G da Fig. 8-35(a). Ele tem quatro vértices, A, B, C, D. Pelo Teorema 8.13, ele tem $H = 3!/2 = 3$ circuitos hamiltonianos. Assumindo que os circuitos começam no vértice A, o que se segue são três circuitos e seus pesos.

$$|ABCDA| = 3 + 5 + 6 + 7 = 21$$
$$|ACDBA| = 2 + 6 + 9 + 3 = 20$$
$$|ACBDA| = 2 + 5 + 9 + 7 = 23$$

(a)

	P	Q	R	S	T
P		18	22	15	20
Q	18		11	12	22
R	22	11		16	10
S	15	12	16		13
T	20	22	10	13	

(b)

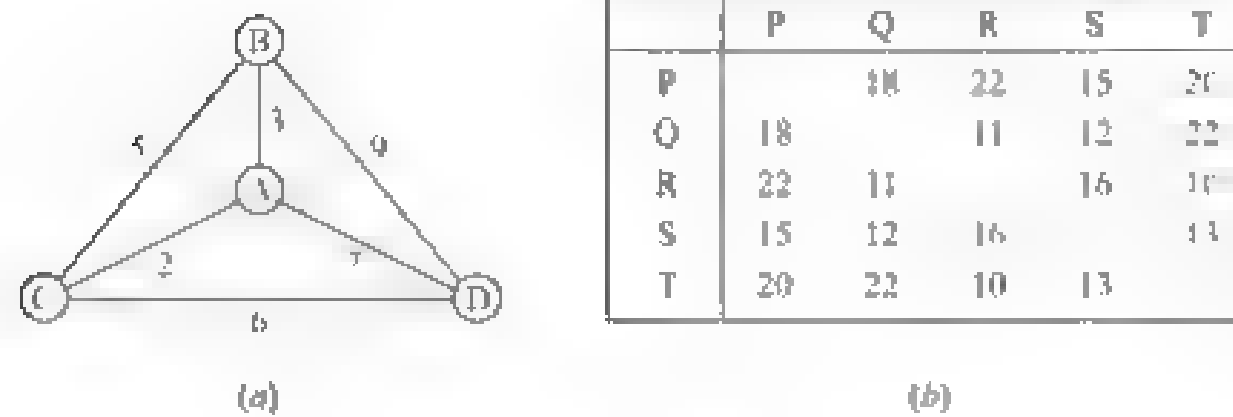



Figura 8-35

Assim, $ACDBA$ com peso 20 é o circuito hamiltoniano de peso mínimo.

Resolvemos o "problema do caixeiro viajante" para o grafo completo ponderado da Fig. 8-35(a), listando e encontrando os pesos de seus três possíveis circuitos hamiltonianos. No entanto, para um grafo com muitos vértices isso pode não ser prático ou mesmo impossível. Por exemplo, um grafo completo com 15 vértices tem mais de 40 milhões de circuitos hamiltonianos. Consequentemente, para circuitos com muitos vértices, uma estratégia de algum tipo é necessária para resolver ou apresentar uma solução aproximada para o problema do caixeiro viajante. Discutimos um dos mais simples algoritmos aqui.

Algoritmo do vizinho mais próximo

O algoritmo do vizinho mais próximo, iniciando em um dado vértice, escolhe a aresta com o menor peso para o próximo vértice possível, ou seja, o vértice "mais próximo". Essa estratégia é continuada em cada vértice sucessivo até um circuito hamiltoniano ser completado.

Exemplo 8.6 Seja G o grafo ponderado dado pela tabela da Fig. 8-35(b). Isto é, G tem os vértices $P, Q, \ldots, T$, e a distância de P a Q é 18, de P a R é 22, e assim por diante, até a distância de T a S de 13. Aplicamos o algoritmo do vizinho mais próximo em G, começando em: (a) P, (b) Q.

(a) Iniciando em P, a primeira linha da tabela nos mostra que o vértice mais próximo de P é S com distância 15. A quarta linha mostra que o vértice mais próximo de S é Q com distância 12. O vértice mais próximo de Q é R com distância 11. A partir de R, não há escolha a não ser ir para T com distância 10. Finalmente, a partir de T, não há escolha a não ser voltar para P com distância 20. Consequentemente, o algoritmo do vizinho mais próximo, começando em P, conduz ao seguinte circuito hamiltoniano ponderado:

$$PSQRTP| = 15 + 12 + 11 + 10 + 20 = 68$$

(b) Iniciando em Q, o vértice mais próximo é R com distância 11, a partir de R, o mais próximo é T com distância 10; e a partir de T, o mais próximo é S com distância 13. A partir de S, devemos ir para P com distância 15, e finalmente, a partir de P, devemos retornar para Q com distância 18. Logo, o algoritmo do vizinho mais próximo, iniciando em Q, conduz ao seguinte circuito hamiltoniano ponderado.

$$|QRTSPQ| = 11 + 10 + 13 + 15 + 18 = 67$$

A ideia por trás do algoritmo do vizinho mais próximo é reduzir o peso total, minimizando o peso em cada passo. A despeito de isso parecer razoável, o Exemplo 8.6 mostra que podemos não obter um circuito hamiltoniano de peso mínimo; ou seja, não pode ser ambos 68 e 67. Apenas verificando todos os $H = (n - 1)!/2 = 12$ circuitos hamiltonianos de G é que realmente conheceremos aquele com peso mínimo. De fato, o algoritmo do vizinho mais próximo começando em A, na Fig. 8-35(a), leva ao circuito $ACBDA$ que tem o peso máximo. Contudo, o algoritmo do vizinho mais próximo em geral dá um circuito hamiltoniano que é relativamente próximo àquele com peso mínimo.

Problemas Resolvidos

Terminologia para grafos

8.1 Considere o grafo G na Fig. 8-36(a).

(a) Descreva G formalmente, ou seja, encontre o conjunto $V(G)$ de vértices de G e o conjunto $E(G)$ de arestas de G.

(b) Encontre o grau de cada vértice e verifique o Teorema 8.1 para esse grafo.

(a) Há cinco vértices. Logo, $V(G) = \{A, B, C, D, E\}$. Existem sete pares $\{x, y\}$ de vértices onde o vértice x é conectado com y; logo,

$$E(G) = [\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, E\}, \{C, D\}, \{C, E\}]$$

(b) O grau de um vértice é igual ao número de arestas aos quais ele pertence; por exemplo, $\deg(A) = 3$, uma vez que A pertence às arestas $\{A, B\}$, $\{A, C\}$ e $\{A, D\}$. Analogamente,

$$\deg(B) = 3, \deg(C) = 4, \deg(D) = 2, \deg(E) = 2$$

A soma dos graus é $3 + 3 + 4 + 2 + 2 = 14$, que é o dobro do número de arestas.

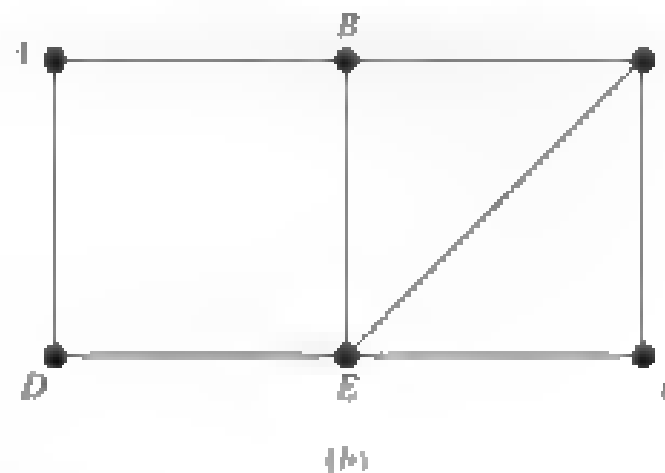
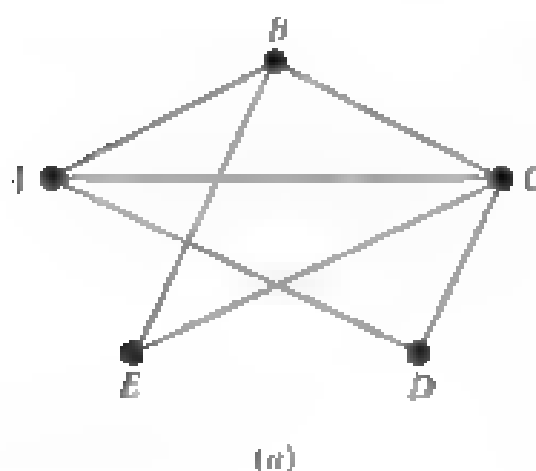



Figura 8-36

8.2 Considere o grafo G na Fig. 8-36(b). Encontre:

(a) todos os caminhos simples de A a F;
(b) todas as trilhas de A a F;
(c) $d(A, F)$, a distância de A a F;
(d) diam (G), o diâmetro de G;
(e) todos os ciclos que incluem o vértice A,
(f) todos os ciclos de G.

(a) Um caminho simples de A a F é um caminho tal que nenhum vértice e, consequentemente, nenhuma aresta, é repetido. Há sete caminhos assim, quatro começando com a aresta $\{A, B\}$ e três começando com a aresta $\{A, D\}$

$$(A, B, C, F), (A, B, C, E, F), (A, B, E, F), (A, B, E, C, F),$$
$$(A, D, E, F), (A, D, E, B, C, F), (A, D, E, C, F).$$

(b) Uma trilha de A a F é um caminho tal que nenhuma aresta é repetida. Há nove trilhas: os sete caminhos simples de (a) e

$$(A, D, E, B, C, E, F) \text{ e } (A, D, E, C, B, E, F)$$

(c) Existe um caminho, por exemplo, (A, B, C, F), de A a F com comprimento 3 e nenhum caminho mais curto de A a F; logo, $d(A, F) = 3$.

(d) A distância entre dois vértices quaisquer não é maior do que 3, e a distância de A a F é 3, logo, diam (G) = 3.

(e) Um ciclo é um caminho fechado no qual nenhum vértice é repetido (exceto o primeiro e o último). Existem três ciclos que incluem o vértice A.

$$(A, B, E, D, A), (A, B, C, E, D, A), (A, B, C, F, E, D, A).$$

(*f*) Há seis ciclos em G; os três em (*e*) e

$$(B, C, E, B), (C, F, E, C), (B, C, F, E, B)$$

8.3 Considere os multigrafos na Fig. 8-37.

(*a*) Quais deles são conexos? Se um grafo não é conexo, encontre suas componentes conexas.

(*b*) Quais são acíclicos (sem ciclos)?

(*c*) Quais são livres de laços (sem laços)?

(*d*) Quais são grafos (simples)?

(*a*) Apenas (1) e (3) são conexos, (2) é desconexo, suas componentes conexas são $\{A, D, E\}$ e $\{B, C\}$. (4) é desconexo, suas componentes conexas são $\{A, B, E\}$ e $\{C, D\}$.

(*b*) Somente (1) e (4) são acíclicos. (2) tem o ciclo (A, D, E, A) e (3) tem o ciclo (A, B, E, A).

(*c*) Apenas (4) tem um laço, que é $\{B, B\}$.

(*d*) Somente (1) e (2) são grafos. O multigrafo (3) tem arestas múltiplas $\{A, E\}$ e $\{A, E\}$, e (4) tem arestas múltiplas $\{C, D\}$ e $\{C, D\}$ e um laço $\{B, B\}$.

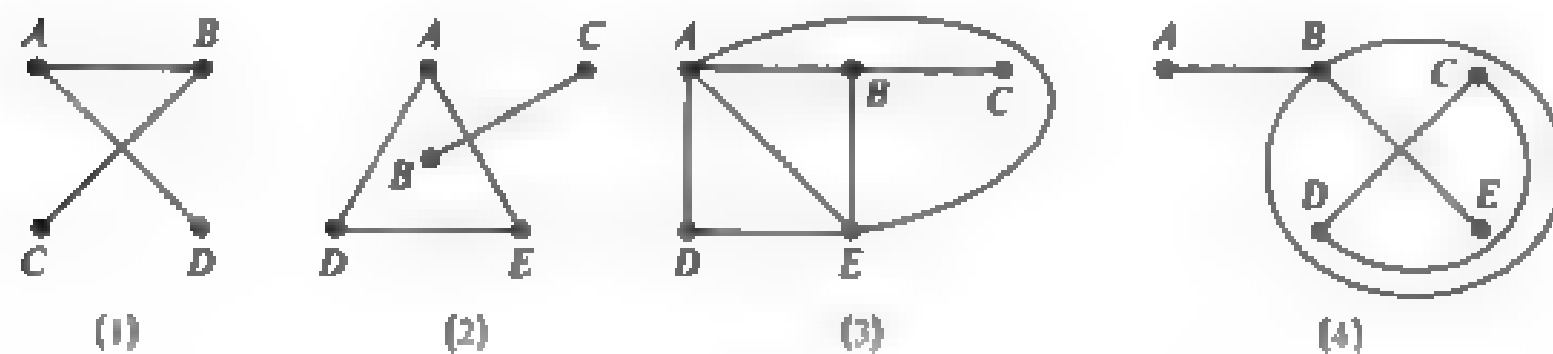



Figura 8-37

8.4 Seja G um grafo na Fig. 8-38(*a*). Encontre:

(*a*) todos os caminhos simples de A a C; (*d*) $G - Y$;

(*b*) todos os ciclos; (*e*) todos os pontos de corte;

(*c*) o subgrafo H gerado por $V' = \{B, C, X, Y\}$; (*f*) todas as pontes.

(*a*) Há dois caminhos simples de A a C: (A, X, Y, C) e (A, X, B, Y, C).

(*b*) Há apenas um ciclo: (B, X, Y, B).

(*c*) Como mostrado na Fig. 8-38(*b*), H consiste nos vértices V' e no conjunto E' de todas as arestas cujos pontos terminais pertencem a V', ou seja, $E' = [\{B, X\}, \{X, Y\}, \{B, Y\}, \{C, Y\}]$.

(*d*) Delete o vértice Y de G e todas as arestas que contêm Y, para obter o grafo $G - Y$ na Fig. 8-38(*c*). (Observe que Y é um ponto de corte, uma vez que $G - Y$ é desconexo.)

(*e*) Os vértices A, X e Y são pontos de corte.

(*f*) Uma aresta e é uma ponte se $G - e$ for desconexo. Assim, há três pontes: $\{A, Z\}$, $\{A, X\}$ e $\{C, Y\}$.

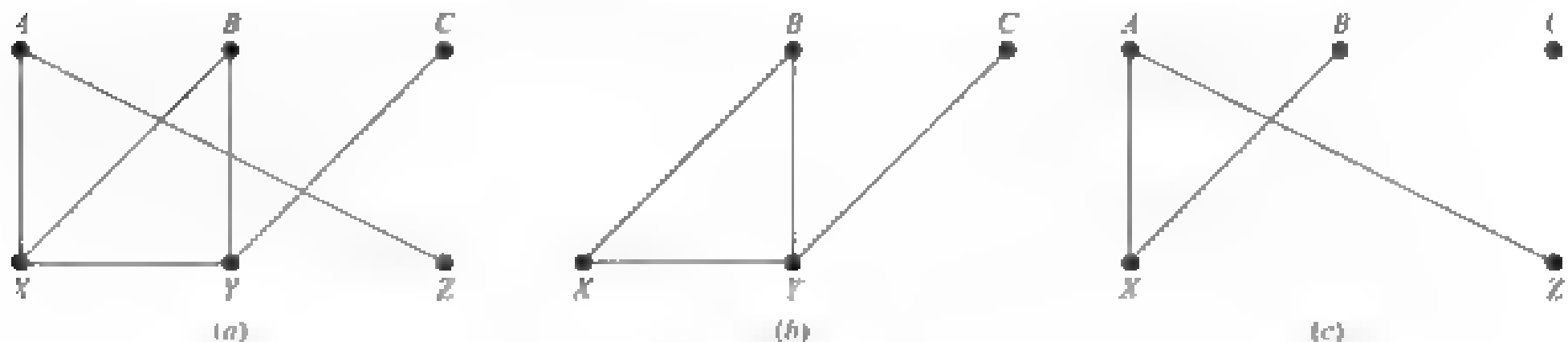



Figura 8-38

8.5 Considere o grafo G na Fig. 8-36(b). Encontre os subgrafos obtidos quando cada vértice é deletado. G apresenta pontos de corte?

Quando eliminamos um vértice de G, temos que deletar também todas as arestas que contêm o vértice. Os seis grafos obtidos, deletando cada um dos vértices de G, são mostrados na Fig. 8-39. Todos os seis grafos são conexos, logo, nenhum vértice é ponto de corte.

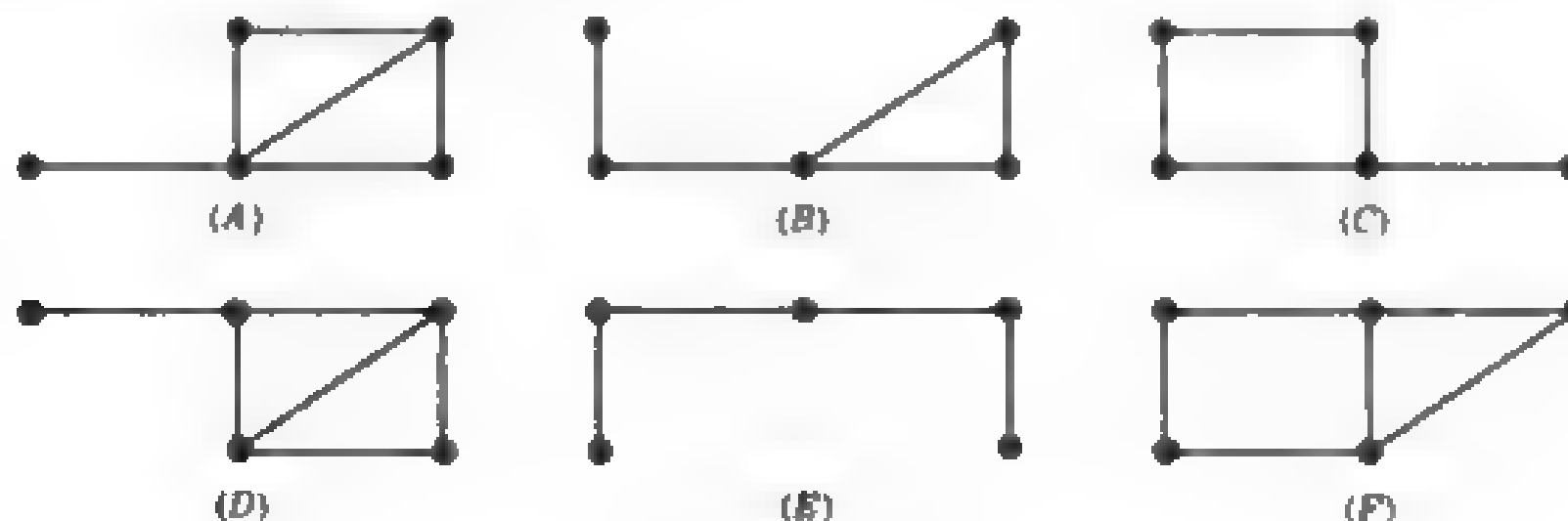



Figura 8-39

8.6 Mostre que os seis grafos obtidos no Problema 8.5 são distintos, ou seja, nenhum par deles é de isomorfos. Também mostre que (B) e (C) são homeomorfos.

Os graus dos cinco vértices de qualquer grafo não podem ser igualados aos graus de qualquer outro grafo, exceto para (B) e (C). Portanto, nenhum dos grafos é isomorfo a outro, exceto, possivelmente (B) e (C).

Contudo, se eliminamos o vértice de grau 3 em (B) e (C), obtemos subgrafos distintos. Assim, (B) e (C) são também não isomorfos. Porém, (B) e (C) são homeomorfos, pois eles podem ser obtidos a partir de grafos isomorfos, acrescentando-se vértices apropriados.

Grafos atravessáveis, circuitos de Euler e hamiltonianos

8.7 Considere cada grafo na Fig. 8-40. Quais deles são atravessáveis, ou seja, admitem caminhos de Euler? Quais são eulerianos, isto é, têm um circuito de Euler? Para aqueles que não têm, explique o porquê.

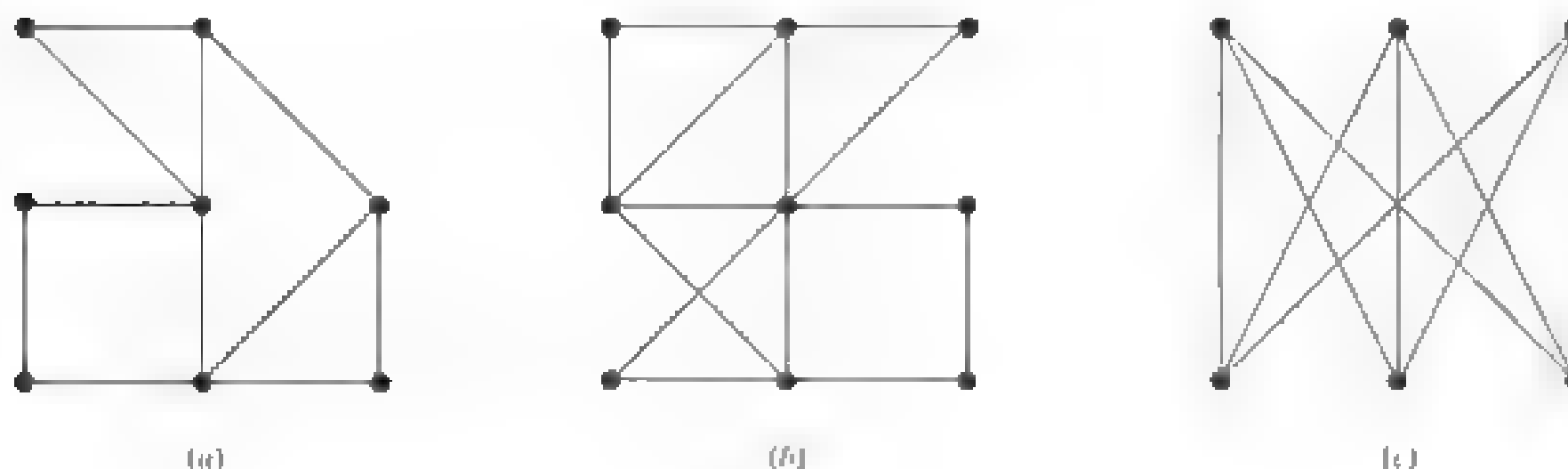



Figura 8-40

G é atravessável (tem um caminho de Euler) se somente 0 ou 2 vértices têm grau ímpar, e G é euleriano (admite um circuito de Euler) se todos os vértices são de grau par (Teorema 8.3).

(a) Atravessável, uma vez que há dois vértices ímpares. O caminho atravessável deve começar em um dos vértices ímpares e terminar no outro.

(b) Atravessável, pois todos os vértices são pares. Assim, G tem um circuito de Euler.

(c) Como seis vértices têm graus ímpares, G não é atravessável.

8.8 Quais dos grafos na Fig. 8-40 têm um circuito hamiltoniano? Se não for o caso, explique por quê.

Os grafos (*a*) e (*c*) têm circuitos hamiltonianos. (O leitor deve ser capaz de facilmente encontrar um deles.) Contudo, o grafo (*b*) não admite circuito hamiltoniano, pois se α é um circuito hamiltoniano, então α deve conectar o vértice do meio com o aquele imediatamente abaixo, em seguida proceder ao longo da linha de baixo para o vértice imediatamente à direita, depois verticalmente para o vértice no meio à direita, mas então ele é forçado a voltar ao vértice central antes de visitar os demais.

8.9 Demonstre o Teorema 8.3 (Euler). Um grafo finito conexo G é euleriano se, e somente se, cada vértice tem grau par.

Suponha que G é euleriano e T é uma trilha euleriana fechada. Para qualquer vértice v de G, a trilha T entra e sai de v o mesmo número de vezes sem repetir qualquer aresta. Logo, v tem um grau par.

Suponha, reciprocamente, que cada vértice de G tem grau par. Construímos uma trilha euleriana. Começamos uma trilha T_1 em qualquer aresta e. Estendemos T_1 adicionando uma aresta após a outra. Se T_1 não for fechado em qualquer passo, digamos, T_1 começa em u, mas termina em $v \neq u$, então apenas um número ímpar das arestas incidentes sobre v aparecem em T_1, logo, podemos estender T_1 por outra aresta incidente sobre v. Assim, podemos continuar a estender T_1 até T_1 retornar ao seu vértice inicial u, ou seja, até T_1 ser fechado. Se T_1 inclui todas as arestas de G, então T_1 é nossa trilha euleriana.

Suponha que T_1 não inclui todas as arestas de G. Considere o grafo H obtido pela eliminação de todas as arestas de T_1 de G. H pode não ser conexo, mas cada vértice de H tem grau par, pois T_1 contém um número par das arestas incidentes sobre qualquer vértice. Como G é conexo, há uma aresta e' de H que tem um ponto extremo u' em T_1. Construímos uma trilha T_2 em H, começando em u' e usando e'. Como todas as arestas em H têm grau par, podem continuar a estender T_2 em H até T_2 retornar a u', como retratado na Fig. 8-41. Podemos claramente colocar T_1 e T_2 juntos para formar uma trilha fechada maior em G. Continuamos esse processo até todas as arestas de G serem usadas. Finalmente, obtemos uma trilha euleriana e, assim, G é euleriano.

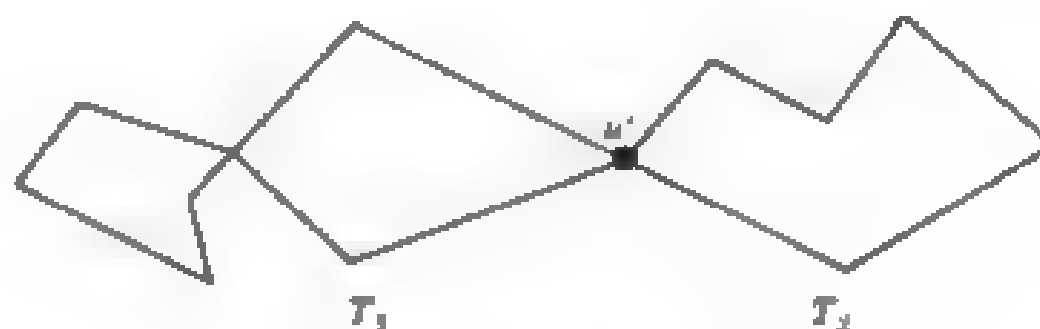



Figura 8-41

Árvores, árvores geradoras

8.10 Esboce todas as árvores com exatamente seis vértices.

Há seis árvores assim, as quais são mostradas na Fig. 8-42. A primeira tem diâmetro 5, as duas seguintes têm diâmetro 4, as outras duas têm diâmetro 3 e a última conta com diâmetro 2. Qualquer outra árvore com seis nós é isomorfa a uma dessas seis.

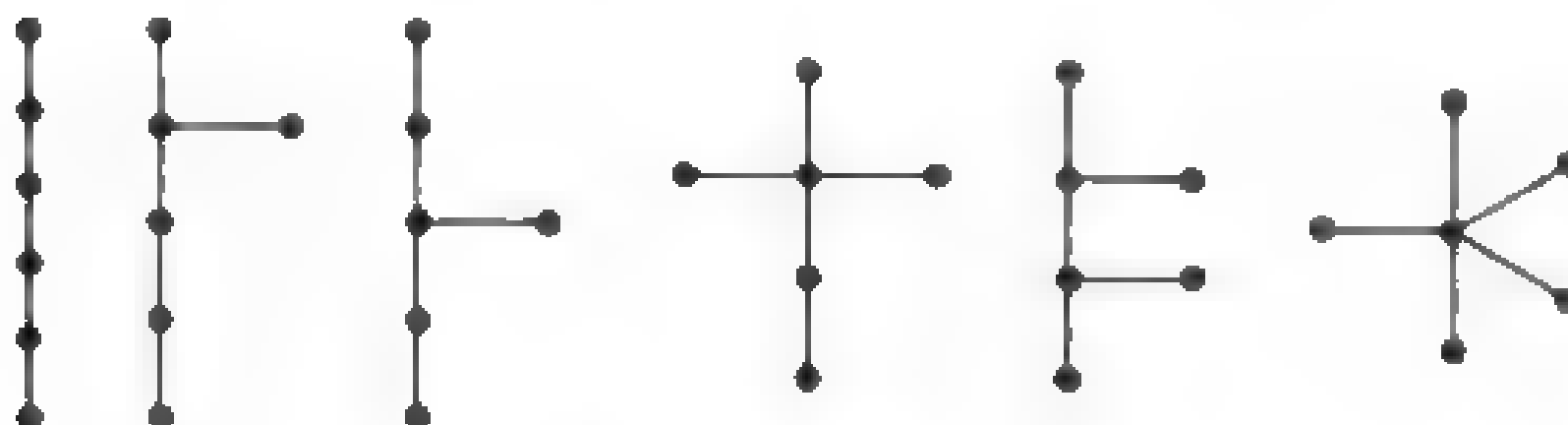



Figura 8-42

8.11 Encontre todas as árvores geradoras do grafo G mostrado na Fig. 8-43(a).

Há oito árvores geradoras como as pedidas, conforme mostrado na Fig. 8-43(b). Cada árvore geradora deve ter $4 - 1 = 3$ arestas, uma vez que G tem quatro vértices. Assim, cada árvore pode ser obtida, eliminando duas das cinco arestas de G. Isso pode ser conseguido de dez maneiras,

(a) Grafo G (b) Árvores geradoras

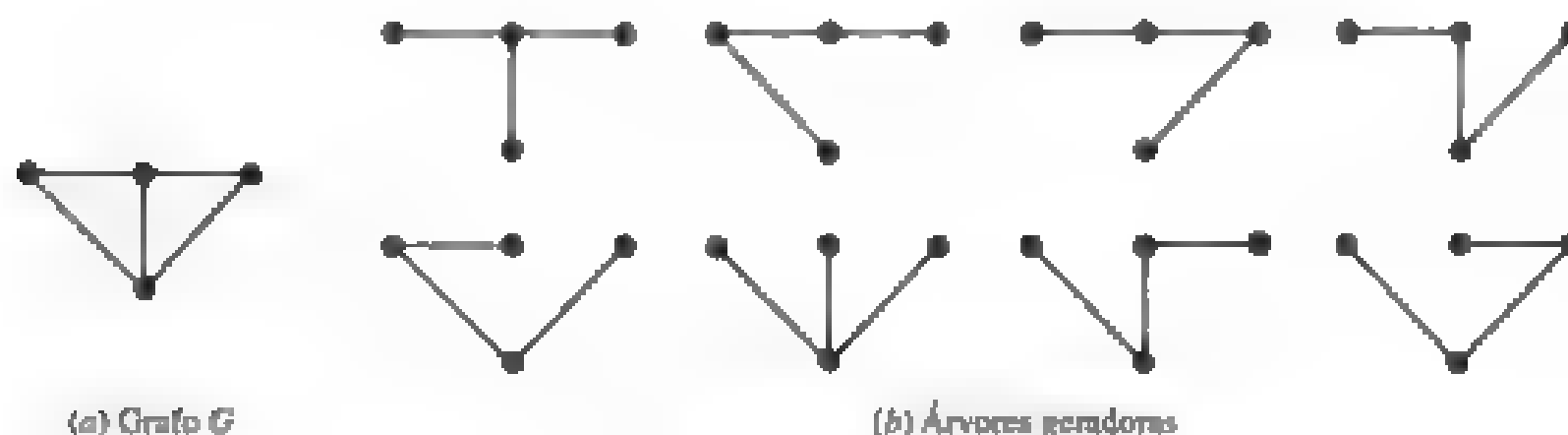



Figura 8-43

exceto que duas das maneiras conduzem a grafos desconexos. Portanto, as oito árvores geradoras acima são todas árvores geradoras de G.

8.12 Encontre a árvore geradora mínima T para o grafo ponderado G na Fig. 8-44(a).

(a)

(b)

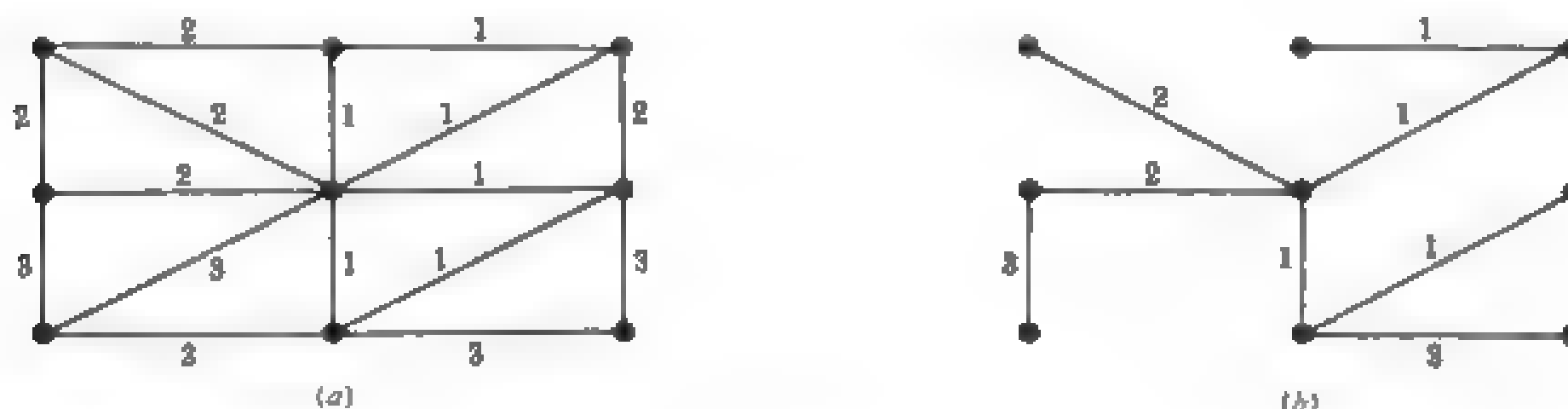



Figura 8-44

Como G tem $n = 9$ vértices, T deve ter $n - 1 = 8$ arestas. Aplique o Algoritmo 8.2, ou seja, continue deletando arestas com comprimento máximo e sem desconectar o grafo até restarem apenas $n - 1 = 8$ arestas. Alternativamente, aplique o Algoritmo 8.3, isto é, começando com os nove vértices, continue adicionando arestas com comprimento mínimo sem formar qualquer ciclo até $n - 1 = 8$ arestas serem acrescentadas. Ambos os métodos fornecem uma árvore geradora mínima, tal como se mostra na Fig. 8-44(b).

8.13 Seja G um grafo com mais de um vértice. Prove que as seguintes afirmações são equivalentes.

(i) G é uma árvore.

(ii) Cada par de vértices é conectado por exatamente um caminho simples.

(iii) G é conexo; mas $G - e$ é desconexo para qualquer aresta e de G.

(iv) G é acíclico, mas se qualquer aresta é adicionada a G, então o grafo resultante tem exatamente um ciclo.

(i) *implica* (ii). Sejam u e v dois vértices de G. Como G é uma árvore, G é conexo. Logo, existe pelo menos um caminho entre u e v. Pelo Problema 8.37, pode haver somente um caminho simples entre u e v. Caso contrário, G contém um ciclo.

(ii) *implica* (iii). Suponha que eliminamos uma aresta $e = \{u, v\}$ de G. Note que e é um caminho de u a v. Suponha que o grafo resultante $G - e$ tem um caminho P de u a v. Então P e e são caminhos distintos de u a v, o que contradiz a hipótese. Logo, não há caminho entre u e v em $G - e$; assim, $G - e$ é desconexo.

(iii) *implica* (iv). Suponha que G contém um ciclo C que tem uma aresta $e = \{u, v\}$. Por hipótese, G é conexo mas $G' = G - e$ é desconexo, com u e v pertencendo a diferentes componentes de G' (Problema 8.41). Isso contradiz o fato de que u e v são conectados pelo caminho $P = C - e$ que está em G'. Logo, G é acíclico. Agora considere x e y como

vértices de G e faça H o grafo obtido pelo acréscimo da aresta $e = \{x, y\}$ a G. Como G é conexo, há um caminho P de x a y em G; logo, $C = P \cup e$ forma um ciclo em H. Suponha que H contém outro ciclo C'. Como G é acíclico, C' deve conter a aresta e, digamos, $C' = P' \cup e$. Então P e P' são dois caminhos simples em G de x a y. (Ver Fig. 8-45.) Pelo Problema 8.37, G contém um ciclo, o que contradiz o fato de que G é acíclico. Logo, H contém apenas um ciclo.

(iv) *implica* (i). Como adicionar qualquer aresta $e = \{x, y\}$ a G produz um ciclo, os vértices x e y já devem estar conectados em G. Logo, G é conexo e, por hipótese, G é acíclico; ou seja, G é uma árvore.

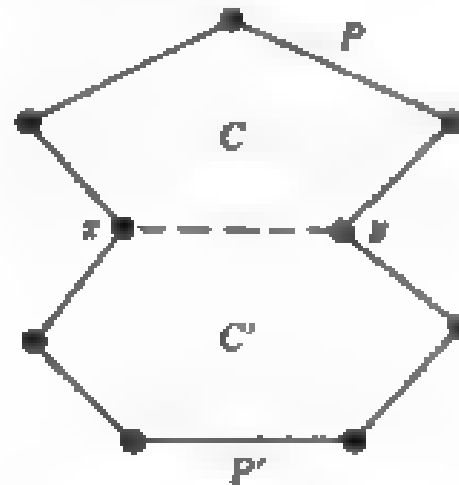



Figura 8-45

8.14 Prove o Teorema 8.6: Seja G um grafo finito com $n \geq 1$ vértices. Então as afirmações a seguir são equivalentes. (i) G é uma árvore, (ii) G é acíclico e tem $n - 1$ arestas, (iii) G é conexo e tem $n - 1$ arestas.

A demonstração é por indução em n. O teorema é certamente verdadeiro para o grafo com apenas um vértice e, portanto, sem arestas. Ou seja, o teorema vale para $n = 1$. Agora assumimos que $n > 1$ e que o teorema vale para grafos com menos do que n vértices.

(i) *implica* (ii). Suponha que G é uma árvore. Então G é acíclico e, assim, só precisamos mostrar que G tem $n - 1$ arestas. Pelo Problema 8.38, G tem um vértice de grau 1. Deletando este vértice e sua aresta, obtemos uma árvore T que tem $n - 1$ vértices. O teorema vale para T. Logo, T tem $n - 2$ arestas. Portanto, G tem $n - 1$ arestas.

(ii) *implica* (iii). Suponha que G é acíclico e tem $n - 1$ arestas. Só precisamos mostrar que G é conexo. Suponha que G é desconexo e tem k componentes, $T_1, \ldots, T_k$, as quais são árvores, uma vez que cada componente é conexa e acíclica. Digamos que T_i tem n_i vértices. Observe que $n_i < n$. Logo, o teorema vale para T_i e, assim, T_i tem $n_i - 1$ arestas. Portanto,

$$n = n_1 + n_2 + \cdots + n_k$$

e

$$n - 1 = (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) = n_1 + n_2 + \cdots + n_k - k = n - k$$

Logo, $k = 1$. Mas isso contradiz a hipótese de que G é desconexo e tem $k > 1$ componentes. Então, G é conexo.

(iii) *implica* (i). Suponha que G é conexo e tem $n - 1$ arestas. Só precisamos mostrar que G é acíclico. Suponha que G tem um ciclo contendo uma aresta e. Deletando e, obtemos o grafo $H = G - e$, que é também conexo. Mas H tem n vértices e $n - 2$ arestas, e isso contradiz o Problema 8.39. Logo, G é acíclico e, portanto, uma árvore.

Grafos planares

8.15 Esboce uma representação plana, se possível, dos grafos (*a*), (*b*) e (*c*) na Fig. 8-46.

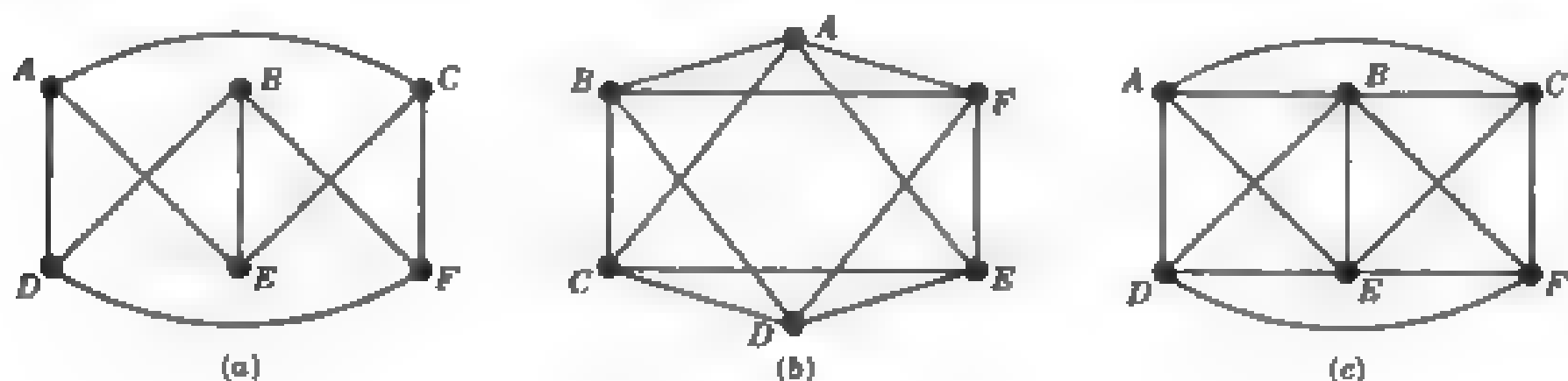



Figura 8-46

(*a*) Redesenhando as posições de *B* e *E*, obtemos uma representação plana do grafo, como na Fig. 8-47(*a*).

(*b*) Esse não é o grafo estrela K_5. Ele tem uma representação plana, como na Fig. 8-47(*b*).

(*c*) Esse grafo não é planar. O grafo utilidade $K_{3,3}$ é um subgrafo, como mostrado na Fig. 8-47(*c*), onde redesenhamos as posições de *C* e *F*.

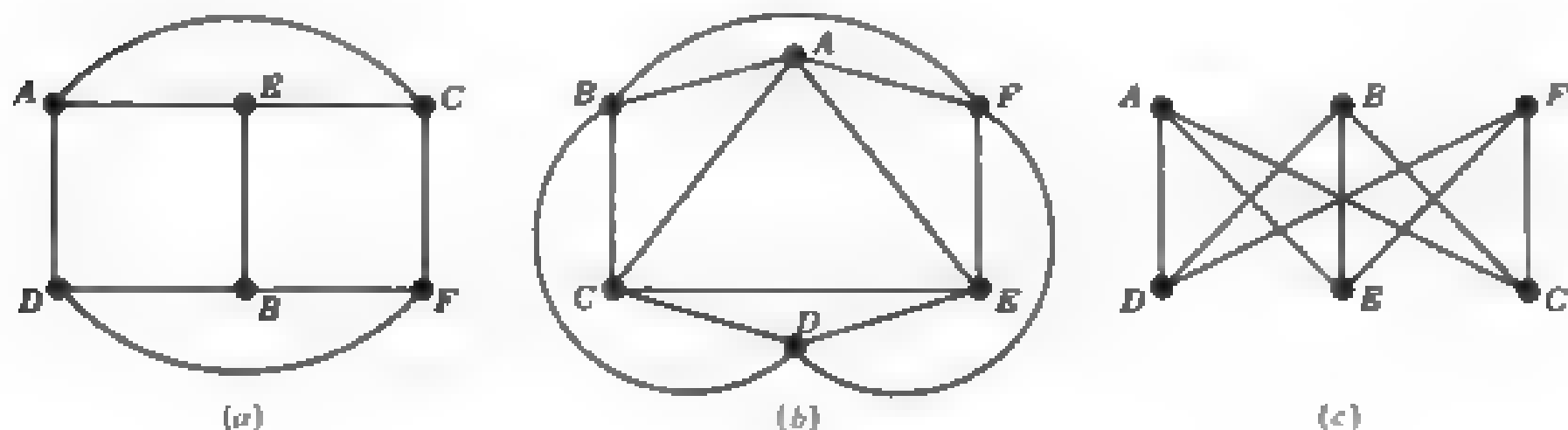



Figura 8-47

8.16 Conte o número *V* de vértices, o número *E* de arestas e o número *R* de regiões de cada mapa na Fig. 8-48, e verifique a fórmula de Euler. Encontre também o grau *d* da região externa.

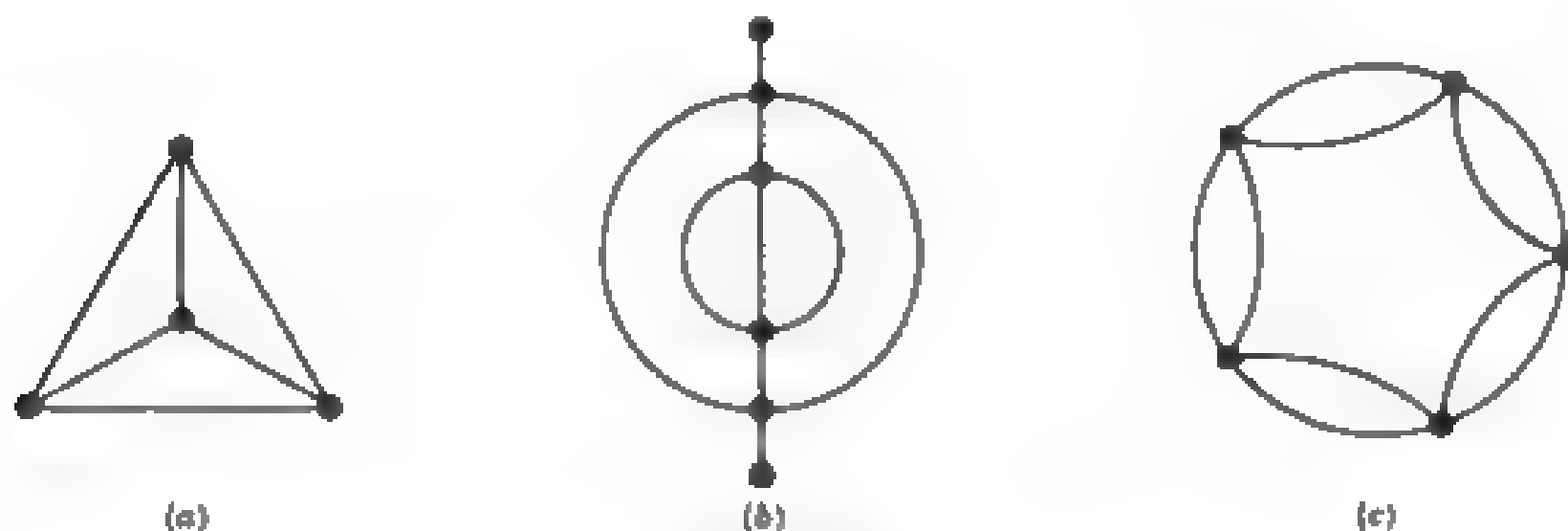



Figura 8-48

(a) $V = 4$, $E = 6$, $R = 4$. Logo, $V - E + R = 4 - 6 + 4 = 2$. Também, $d = 3$.

(b) $V = 6$, $E = 9$, $R = 5$, logo, $V - E + R = 6 - 9 + 5 = 2$. Aqui $d = 6$, pois duas arestas são contadas duas vezes.

(c) $V = 5$, $E = 10$, $R = 7$. Logo, $V - E + R = 5 - 10 + 7 = 2$. Aqui $d = 5$.

8.17 Encontre o número mínimo *n* de cores necessárias para pintar cada mapa na Fig. 8-48.

(a) $n = 4$; (b) $n = 3$; (c) $n = 2$.

8.18 Prove o Teorema 8.8 (Euler): $V - E + R = 2$.

Suponha que o mapa conexo *M* consiste em um único vértice *P*, como na Fig. 8-49(*a*). Então, $V = 1$, $E = 0$ e $R = 1$. Logo, $V - E + R = 2$. Caso contrário, *M* pode ser construído a partir de um único vértice pelas duas construções a seguir:

(1) Adicione um novo vértice Q_2 e conecte-o a um vértice existente Q_1 por uma aresta que não cruze qualquer aresta existente, como na Fig. 8-49(*b*).

(2) Conecte dois vértices existentes Q_1 e Q_2 por uma aresta *e* que não cruze qualquer aresta existente, como na Fig. 8-49(*c*).

Nenhuma operação muda o valor de $V - E + R$. Logo, *M* tem o mesmo valor de $V - E + R$, quando o mapa consiste em um único vértice, ou seja, $V - E + R = 2$. Assim, o teorema está provado.

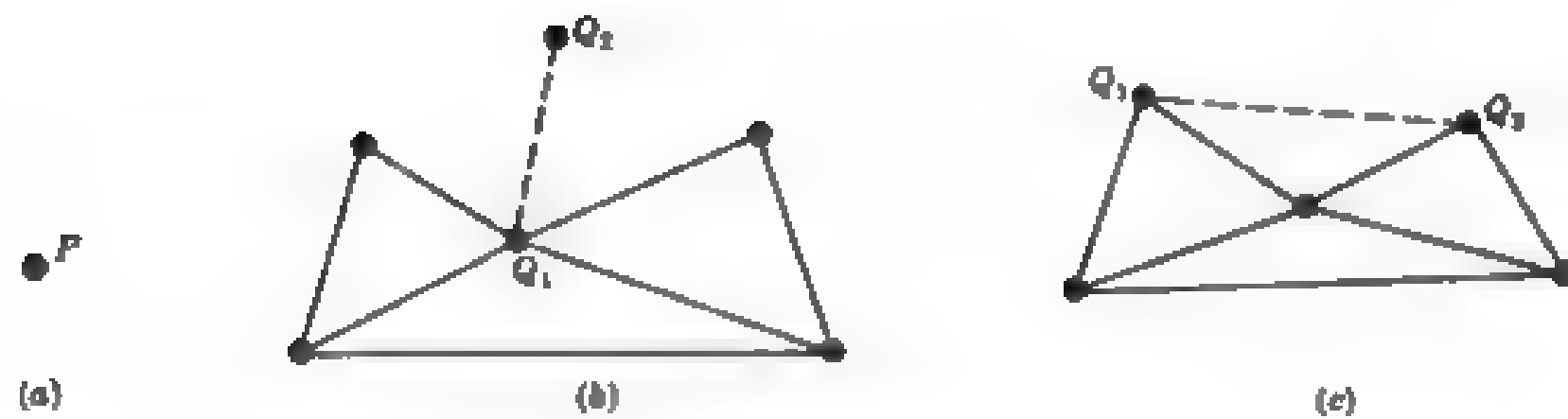



Figura 8-49

8.19 Demonstre o Teorema 8.11. As seguintes afirmações são equivalentes para um grafo G: (i) G é 2-colorível. (ii) G é bipartido. (iii) Todo ciclo de G tem comprimento par.

(i) *implica* (ii). Suponha que G é 2-colorível. Seja M o conjunto de vértices pintados na primeira cor, e seja N o conjunto de vértices pintados na segunda cor. Então M e N formam uma partição bipartida dos vértices de G, uma vez que os vértices de M e os vértices de N não podem ser adjacentes um com o outro, já que são da mesma cor.

(ii) *implica* (iii). Suponha que G é bipartido e M e N formam uma partição bipartida dos vértices de G. Se um ciclo começa em um vértice u de, digamos, M, então ele irá a um vértice de N e, depois, a um vértice de M e, em seguida, a um vértice de N, e assim por diante. Logo, quando o ciclo retorna a u, deve ter comprimento par. Isto é, todo ciclo de G tem comprimento par.

(iii) *implica* (i). Por último, suponha que todo ciclo de G tem comprimento par. Escolhemos um vértice em cada componente conexa e o pintamos na primeira cor, digamos, vermelho. Em seguida, sucessivamente pintamos todos os vértices como se segue. Se um vértice é pintado de vermelho, então qualquer vértice adjacente deve ser pintado na segunda cor, digamos, azul. Se um vértice é pintado de azul, então qualquer vértice adjacente deve ser pintado de vermelho. Como todo ciclo tem comprimento par, nenhum par de vértices adjacentes será pintado da mesma cor. Portanto, G é 2-colorível e o teorema está provado.

8.20 Demonstre o Teorema 8.12: Um grafo planar G é 5-colorível.

A demonstração é por indução sobre o número p de vértices de G. Se $p \leq 5$, então o teorema obviamente vale. Suponha que $p > 5$, e que o teorema vale para grafos com menos de p vértices. Pelo problema anterior, G tem um vértice v tal que $\deg(v) \leq 5$. Por indução, o subgrafo $G - v$ é 5-colorível. Assuma tal coloração. Se os vértices adjacentes a v usam menos do que as cinco cores, então simplesmente pintamos v com uma das cores restantes e obtemos uma 5-coloração de G. Ainda resta o caso em que v é adjacente a cinco vértices que são pintados em cores distintas. Digamos que os vértices, movendo em sentido anti-horário em torno de v, são $v_1, \ldots, v_5$, os quais são pintados, respectivamente, pelas cores $c_1, \ldots, c_5$. (Ver Fig. 8-50(a).)

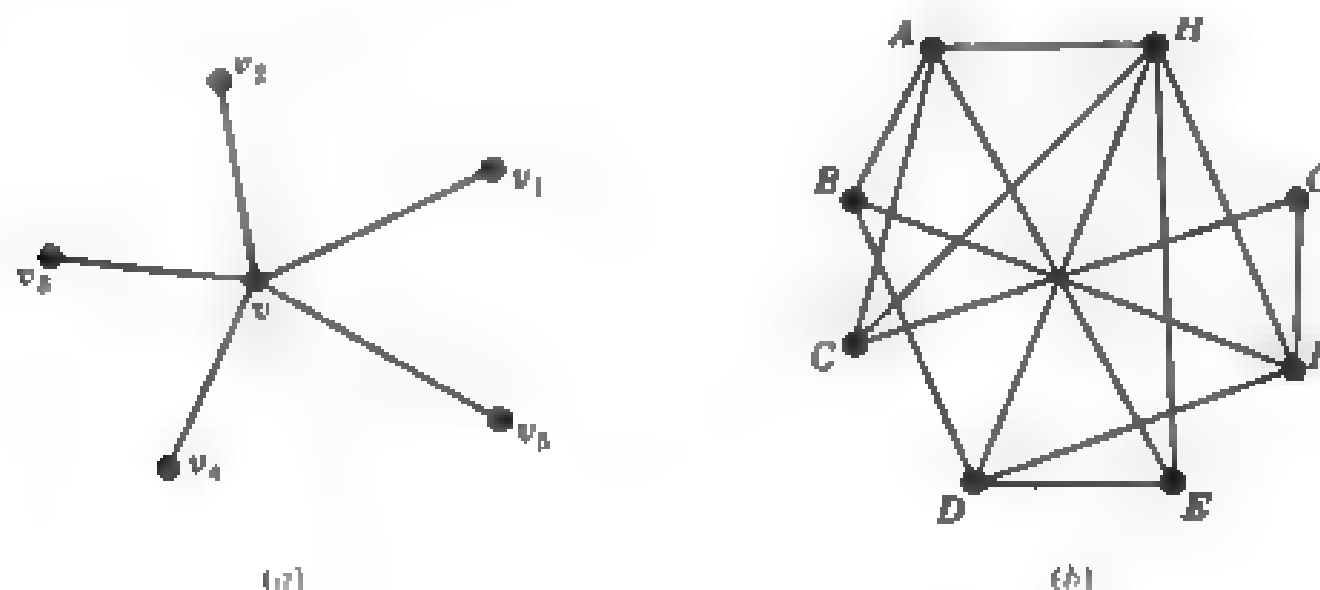



Figura 8-50

Considere agora o subgrafo H de G gerado pelos vértices pintados de c_1 e c_3. Observe que H inclui v_1 e v_3. Se v_1 e v_3 pertencem a diferentes componentes de H, então podemos intercambiar as cores c_1 e c_3 na componente contendo

v_1 sem destruir a coloração de $G - v$. Então, v_1 e v_3, que são pintados por c_3 e c_1, podem ser escolhidos para pintar v, e temos uma 5-coloração de G. Por outro lado, suponha que v_1 e v_3 estão na mesma componente de H. Então existe um caminho P de v_1 a v_3, cujos vértices são pintados de c_1 ou c_3. O caminho P, junto com as arestas $\{v, v_1\}$ e $\{v, v_3\}$, forma um ciclo C que engloba v_2 ou v_4. Considere agora o subgrafo K gerado pelos vértices pintados com c_2 ou c_4. Como C engloba v_2 ou v_4, mas não ambos, os vértices v_2 e v_4 pertencem a diferentes componentes de K. Logo, podemos intercambiar as cores c_2 e c_4 na componente contendo v_2 sem destruir a coloração de $G - v$. Então, v_2 e v_4 são pintados por c_4, e podemos escolher c_2 para pintar v e obter uma 5-coloração de G. Assim, G é 5-colorível e o teorema foi provado.

8.21 Use o Algoritmo de Welch-Powell 8.4 (Fig. 8-24) para pintar o grafo na Fig. 8-50(*b*).

Primeiro ordene os vértices de acordo com graus decrescentes para obter a sequência

$$H, A, D, F, B, C, E, G$$

Procedendo sequencialmente, usamos a primeira cor para pintar os vértices H e B, depois, G. (Não podemos pintar A, D ou F com a primeira cor, pois cada um é conectado a H, e não podemos pintar C ou E com a primeira cor, uma vez que cada um é conectado a H ou B.) Procedendo sequencialmente com os vértices não pintados, empregamos a segunda cor para pintar os vértices A e D. Os outros vértices F, C e E podem ser coloridos com a terceira cor. Assim, o número cromático n não pode ser maior do que 3. Contudo, em qualquer coloração, H, D e E devem ser pintados com cores distintas, pois eles são conectados um ao outro. Logo, $n = 3$.

8.22 Seja G um grafo planar conexo finito com pelo menos três vértices. Mostre que G tem pelo menos um vértice de grau menor ou igual a 5.

Sejam p o número de vértices e q o número de arestas de G, e suponha que $\deg(u) \geq 6$ para cada vértice u de G. Mas $2q$ é igual à soma dos graus dos vértices de G (Teorema 8.1); logo, $2q \geq 6p$. Portanto,

$$q \geq 3p > 3p - 6$$

Isso contradiz o Teorema 8.9. Logo, algum vértice de G tem grau menor ou igual a 5.

Representação sequencial de grafos

8.23 Encontre a matriz de adjacência $A = [a_{ij}]$ de cada grafo G na Fig. 8-51.

(*a*)

(*b*)

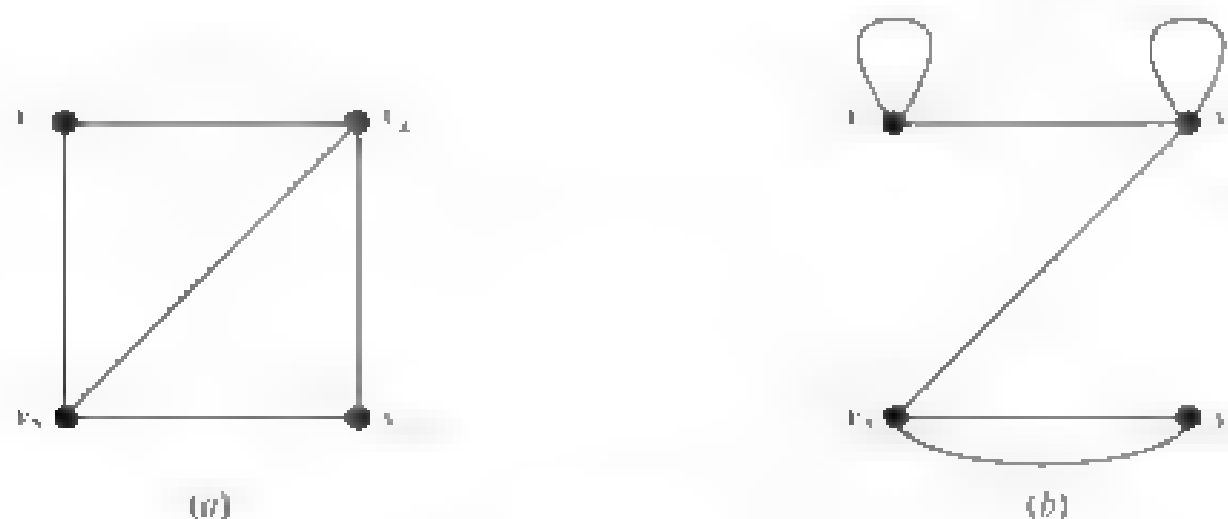



Figura 8-51

Faça $a_{ij} = n$ se há n arestas $\{v_i, v_j\}$ e $a_{ij} = 0$ no caso contrário. Logo:

$$(a)\ A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}; \quad (b)\ A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

(Como (*a*) não tem arestas múltiplas nem laços, as entradas de A são 0 ou 1, e são nulas na diagonal.)

8.24 Esboce o grafo G correspondente a cada matriz de adjacência:

$$(a)\ A = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \qquad (b)\ A = \begin{bmatrix} 1 & 3 & 0 & 0 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

(*a*) Como A é uma matriz quadrada de ordem 5, G tem cinco vértices, digamos, $v_1, v_2, \ldots, v_5$. Esboce uma aresta de v_i a v_j quando $a_{ij} = 1$. O grafo aparece na Fig. 8-52(*a*).

(*b*) Como A é uma matriz quadrada de ordem 4, G tem quatro vértices, digamos, $v_1, \ldots, v_4$. Desenhe n arestas de v_i a v_j quando $a_{ij} = n$. Além disso, desenhe n laços em v_i quando $a_i = n$. O grafo aparece na Fig. 8-52(*b*).

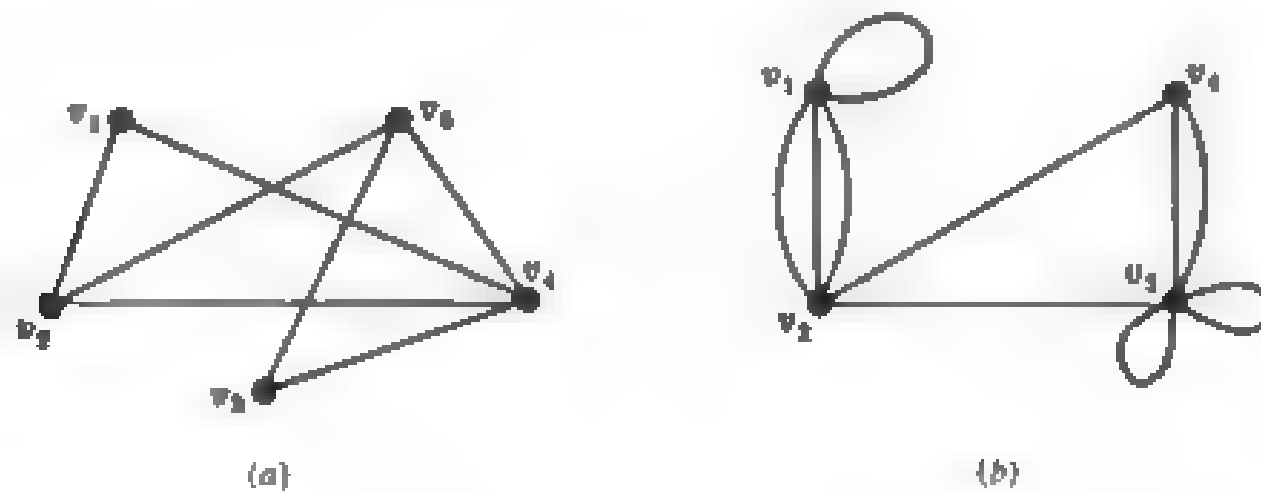



Figura 8-52

8.25 Encontre a matriz de pesos $W = [w_{ij}]$ do grafo ponderado G na Fig. 8-53(*a*), onde os vértices estão armazenados nos DADOS sequenciais como se segue: DADOS: *A, B, C, X, Y*.

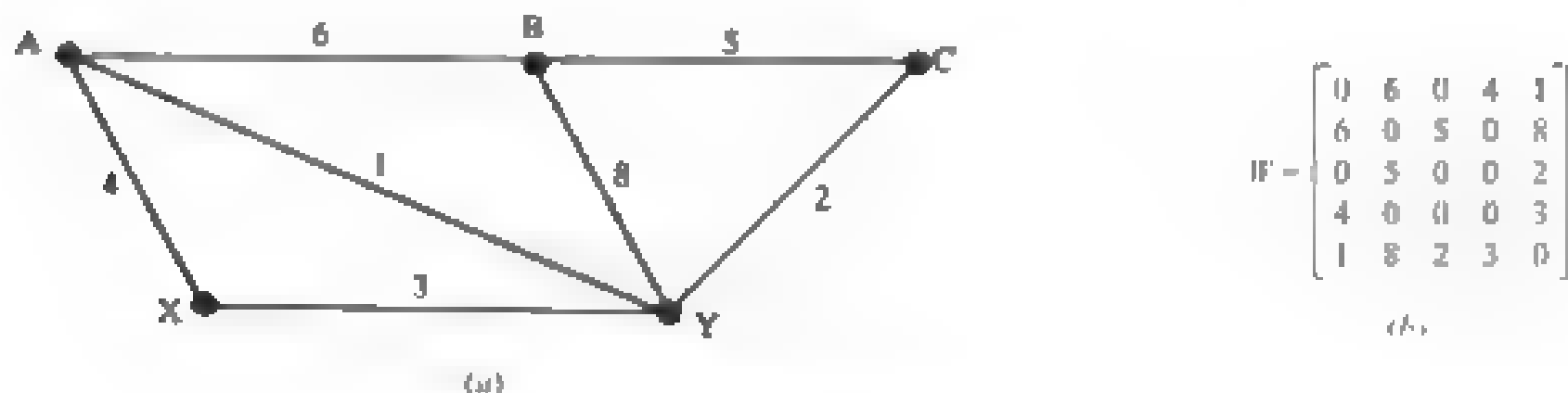



Figura 8-53

Os vértices são numerados de acordo com a maneira como eles estão armazenados nos DADOS sequenciais; logo, $v_1 = A$, $v_2 = B, \ldots, v_5 = Y$. Então faça $W_{ij} = w$, onde w é o peso da aresta de v_i a v_j. Isso conduz à matriz W na Fig. 8-53(b).

Representação ligada de grafos

8.26 Um grafo G com vértices $A, B, \ldots, F$ é armazenado na memória, usando uma representação ligada com um arquivo de vértices e um de arestas, como na Fig. 8-54.

(*a*) Liste os vértices na ordem em que eles aparecem na memória.

(*b*) Encontre a lista de adjacência (v) de cada vértice v de G.

(*a*) Como START = 4, a lista começa com o vértice *D*. NEXT-V nos diz para ir a 1(*B*), depois 3(*F*), em seguida 5(*A*), então 8(*E*) e finalmente 7(*C*); ou seja,

$$D,\ B,\ F,\ A,\ E,\ C$$

(*b*) Aqui $\text{adj}(D) = [5(A), 1(B), 8(E)]$. Especificamente, $\text{PTR}[4(D)] = 7$ e $\text{ADJ}[7] = 5(A)$ nos diz que $\text{adj}(D)$ começa com A. Em seguida, $\text{NEXT}[7] = 3$ e $\text{ADJ}[3] = 1(B)$ nos diz que B é o próximo vértice em $\text{adj}(D)$. Então, $\text{NEXT}[3] = 10$ e $\text{ADJ}[10] = 8(E)$ nos diz que E é o próximo vértice em $\text{adj}(D)$. Contudo, $\text{NEXT}[10] = 0$ nos diz que não há mais vizinhos de D. Analogamente,

$$\text{adj}(B) = [A, D], \quad \text{adj}(F) = [E], \quad \text{adj}(A) = [B, D], \quad \text{adj}(E) = [C, D, F], \quad \text{adj}(C) = [E]$$

Em outras palavras, o que se segue é a estrutura de adjacência de G:

$$G = [A{:}B, D; \quad B{:}A, D; \quad C{:}E; \quad D{:}A, B, E; \quad E{:}C, D, F; \quad F{:}E]$$

Arquivo de vértices

	1	2	3	4	5	6	7	8
VERTEX	*B*		*F*	*D*	*A*		*C*	*E*
NEXT-V	3		5	1	8		0	7
PTR	9		4	7	6		5	2

START [4]

Arquivo de arestas

		2	3	4	5	6	7	8	9	10	11	12	13	14
ADJ	4	4	1	8	8	1	5	3	5	8	4	7		
NEXT	8	0	10	0	0	2	3	0	11	0	0	1		

Figura 8-54

8.27 Esboce o diagrama do grafo G cuja representação ligada aparece na Fig. 8-54.

Use a lista de vértices obtida no Problema 8.26(a) e as listas de adjacência conseguidas no Problema 8.26(b) para desenhar o grafo G na Fig. 8-55.

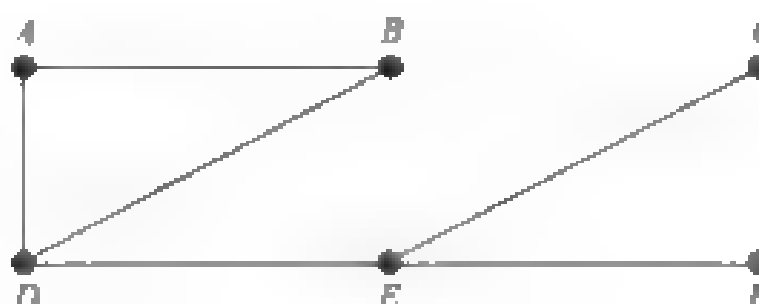



Figura 8-55

8.28 Exiba a estrutura de adjacência (AS) do grafo G em: (*a*) Fig. 8-56(*a*), (*b*) Fig. 8-56(*b*).

A estrutura de adjacência de um grafo G consiste nas listas de adjacência dos vértices, onde usamos dois pontos ":" para separar um vértice de sua lista de adjacência e ponto e vírgula ";" para separar as diferentes listas. Logo:

(*a*) $G = [A{:}B, C, D; B{:}A, C, E; C{:}A, B, D, E; D{:}A, C; E{:}B, C]$

(*b*) $G = [A{:}B, D; B{:}A, C, E; C{:}B, E, F; D{:}A, E; E{:}B, C, D, F; F{:}C, E]$

Algoritmos de grafos

8.29 Considere o grafo G na Fig. 8-56(*a*) (onde os vértices são ordenados alfabeticamente).

(*a*) Encontre a estrutura de adjacência de G.

(*b*) Encontre a ordem na qual os vértices de G são processados, usando um algoritmo DFS (busca em profundidade) que inicia no vértice A.

(a) Liste os vizinhos de cada vértice como se segue:

$$G = [A:B, C, D;\ B:A, J;\ C:A;\ D:A, K;\ J:B, K, M;\ K:D, J, L;\ L:K, M;\ M:J, L]$$

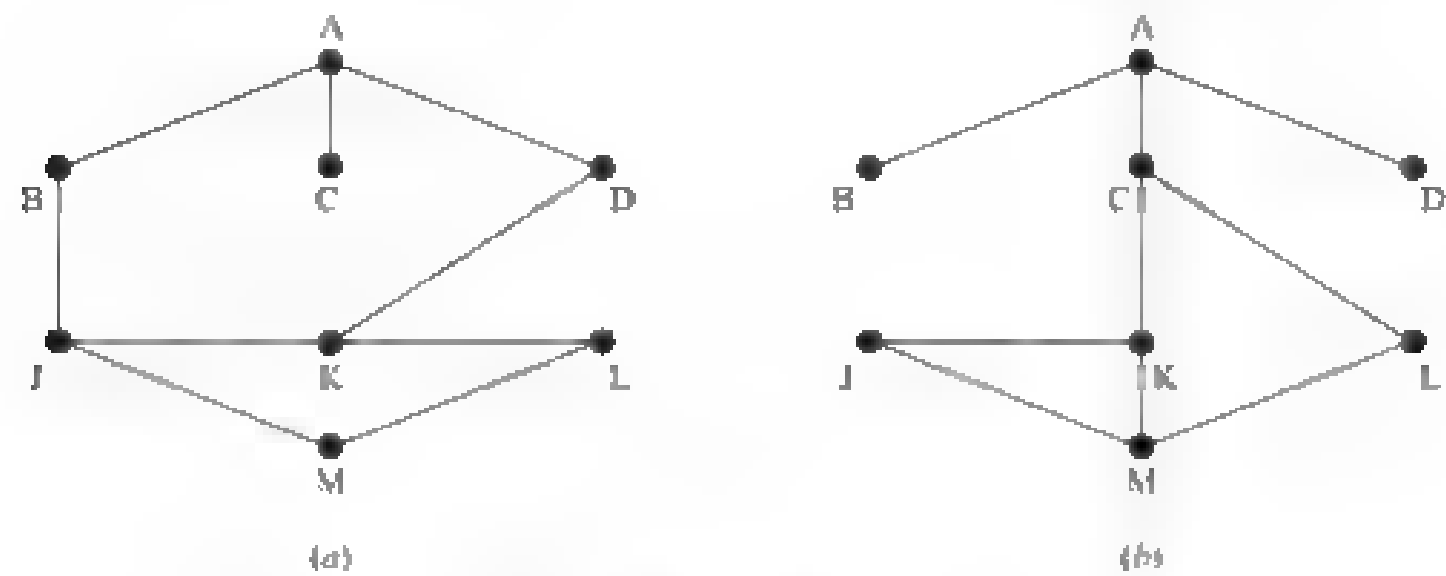



Figura 8-56

(*b*) Durante o algoritmo DFS, o primeiro vértice *N* em PILHA é processado e os vizinhos de *N* (que não foram anteriormente processados) são então jogados em PILHA. No começo, o vértice inicial *A* é jogado em PILHA. O que se segue mostra a sequência de listas de espera em PILHA e os vértices sendo processados:

PILHA	*A*	*DCB*	*KCB*	*LJCB*	*MJCB*	*JCB*	*CB*	*B*	∅
Vértice	*A*	*D*	*K*	*L*	*M*	*J*	*C*	*B*	

Em outras palavras, os vértices são processados na ordem: *A, D, K, L, M, J, C, B*

8.30 Repita o Problema 8.29 para o grafo *G* na Fig. 8-56(*b*).

(*a*) Liste os vizinhos de cada vértice como se segue:

$$G = [A:B, C, D;\ B:A;\ C:A, K, L;\ D:A;\ J:K, M;\ K:C, J, M;\ L:C, M;\ M:J, K, L]$$

(*b*) A seguir, temos a sequência de listas de espera em PILHA e os vértices sendo processados.

PILHA	*A*	*DCB*	*CB*	*LKB*	*MKB*	*KJB*	*JB*	*B*	∅
Vértice	*A*	*D*	*C*	*L*	*M*	*K*	*J*	*B*	

Em outras palavras, os vértices são processados na ordem: *A, D, C, L, M, K, J, B*.

8.31 Começando no vértice *A* e usando um algoritmo BFS (busca em largura), encontre a ordem em que os vértices são processados para o grafo *G* (*a*) na Fig. 8-56(*a*), (*b*) na Fig. 8-56(*b*).

(*a*) A estrutura de adjacência de *G* aparece no Problema 8.29. Durante o algoritmo BFS, o primeiro vértice *N* em FILA é processado e os vizinhos de *N* (que não apareceram anteriormente) são então adicionados à FILA. No começo, o vértice inicial *A* é assinalado à FILA. O que se segue mostra a sequência de listas de espera em FILA e os vértices sendo processados.

FILA	*A*	*DCB*	*JDC*	*JD*	*KJ*	*MK*	*LM*	*L*	∅
Vértice	*A*	*B*	*C*	*D*	*J*	*K*	*M*	*L*	

Em outros termos, os vértices são processados na ordem: *A, B, C, D, J, K, M, L*.

(*b*) A estrutura de adjacência de G aparece no Problema 8.30. A seguir, temos a sequência de listas de espera em FILA e os vértices sendo processados:

FILA	A	DCB	DC	LKD	LK	MJL	MJ	M	$\emptyset$
Vértice	A	B	C	D	K	L	J	M	

Em outras palavras, os vértices são processados na ordem: A, B, C, D, K, L, J, M.

Problema do caixeiro viajante

8.32 Aplique o algoritmo do vizinho mais próximo no grafo ponderado completo G da Fig. 8-57, começando no: (*a*) vértice A; (*b*) vértice D.

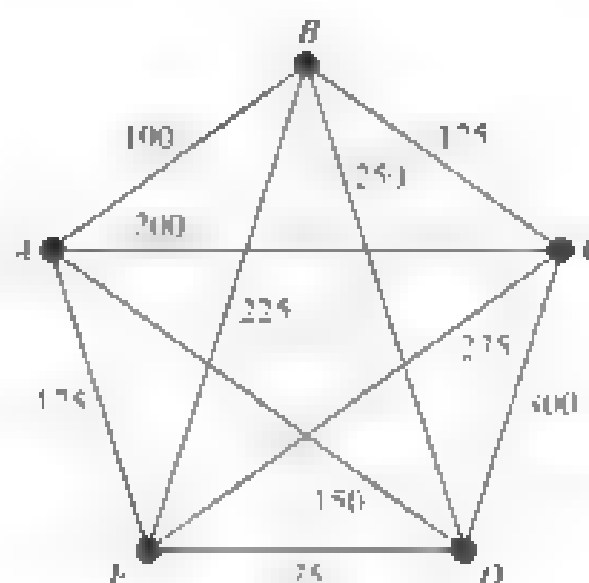



Figura 8-57

(*a*) Começando em A, o vértice mais próximo é B, com distância 100; de B, o mais próximo é C, com distância 125, e de C, o mais próximo é E, com distância de 275. A partir de E, devemos ir para D, com distância de 75, e, finalmente, de D devemos voltar para A, com distância de 150. Consequentemente, o algoritmo de vizinho mais próximo começando em A nos leva ao seguinte circuito hamiltoniano ponderado:

$$|ABCEDA| = 100 + 125 + 275 + 75 + 150 = 725$$

(*b*) Começando em D, devemos ir para E, em seguida A, então B, depois C e finalmente de volta para D. Consequentemente, o algoritmo do vizinho mais próximo iniciando em D nos leva ao seguinte circuito hamiltoniano ponderado:

$$|DEABCD| = 75 + 175 + 100 + 125 + 300 = 775$$

8.33 Prove o Teorema 8.13. O grafo completo K_n com $n \geq 3$ vértices tem $H = (n-1)!/2$ circuitos hamiltonianos.

A convenção de contagem para circuitos hamiltonianos nos permite designar qualquer vértice de um circuito como o ponto de partida. A partir desse ponto, podemos ir a qualquer um dos $n - 1$ vértices e, a partir daí, para qualquer um dos $n - 2$ vértices, e assim por diante, até chegarmos ao último vértice e, em seguida, retornarmos ao ponto inicial. Pelo princípio de contagem básica, há um total de $(n-1)(n-2) \cdots 2 \cdot 1 = (n-1)!$ circuitos que podem ser formados a partir de um ponto inicial. Para $n \geq 3$, qualquer circuito pode fazer par com um no sentido oposto que determina o mesmo circuito hamiltoniano. Consequentemente, há um total de $H = (n-1)!/2$ circuitos hamiltonianos.

Problemas Complementares

Terminologia de grafos

8.34 Considere o grafo G na Fig. 8-58. Encontre:

(a) o grau de cada vértice (e verifique o Teorema 8.1);

(b) todos os caminhos simples de A a L;

(c) todas as trilhas (arestas distintas) de B a C;

(d) $d(A, C)$, a distância de A a C;

(e) diam(G), o diâmetro de G

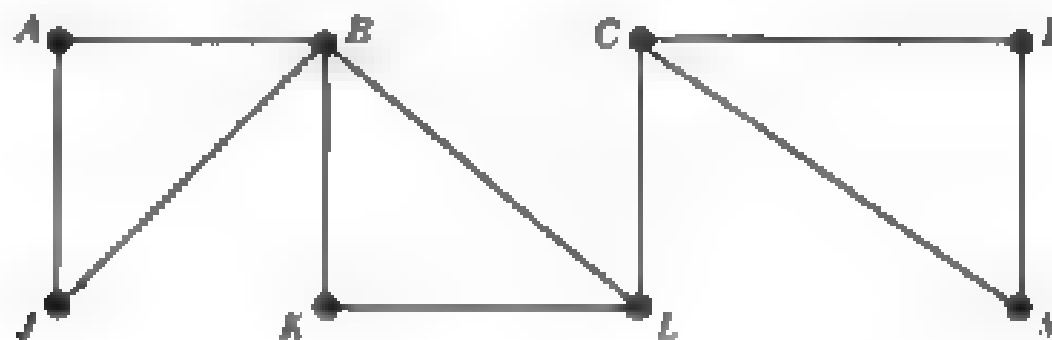



Figura 8-58

8.35 Considere o grafo na Fig. 8-58. Encontre (se houver): (a) todos os ciclos, (b) todos os pontos de corte, (c) todas as pontes.

8.36 Considere o grafo na Fig. 8-58. Encontre o subgrafo $H = H(V', E')$ de G, onde V' é igual a.

(a) $\{B, C, D, J, K\}$ (b) $\{A, C, J, L, M\}$ (c) $\{B, D, J, M\}$ (d) $\{C, K, L, M\}$

Quais deles são isomorfos e quais são homeomorfos?

8.37 Suponha que um grafo G contém dois caminhos distintos de um vértice u a um vértice v. Mostre que G tem um ciclo.

8.38 Suponha que G é um grafo acíclico com pelo menos uma aresta. Mostre que G tem pelo menos dois vértices de grau 1

8.39 Mostre que um grafo conexo G com n vértices deve ter pelo menos $n - 1$ arestas.

8.40 Encontre o número de grafos conexos com quatro vértices. (Esboce-os.)

8.41 Seja G um grafo conexo. Prove:

(a) Se G contém um ciclo C que tem uma aresta e, então $G - e$ ainda é conexo.

(b) Se $e = \{u, v\}$ é uma aresta tal que $G - e$ é desconexo, então u e v pertencem a diferentes componentes de $G - e$

8.42 Suponha que G tem V vértices e E arestas. Sejam M e m, respectivamente, o máximo e o mínimo dos graus dos vértices em G. Mostre que $m \leq 2E/V \leq M$

8.43 Considere os dois passos a seguir em um grafo G: (1) Delete uma aresta. (2) Delete um vértice e todas as arestas que o contém. Mostre que todo subgrafo H de um grafo finito G pode ser obtido por uma sequência consistindo nesses dois passos.

Grafos atravessáveis, circuitos eulerianos e hamiltonianos

8.44 Considere os grafos K_5, $K_{3,3}$ e $K_{2,3}$ na Fig. 8-59. Encontre um caminho euleriano (atravessável) ou um circuito euleriano para cada grafo, se existir. Se não houver, explique por quê.

8.45 Considere cada grafo na Fig. 8-59. Encontre um caminho hamiltoniano ou um circuito hamiltoniano, se existir. Se não houver, explique por quê.

8.46 Mostre que K_n tem $H = (n - 1)!/2$ circuitos hamiltonianos. Encontre, em especial, o número de circuitos hamiltonianos para o grafo K_5 na Fig. 8-59(a).

8.47 Suponha que G e G^* são grafos homeomorfos. Mostre que G é atravessável (euleriano) se, e somente se, G^* é atravessável (euleriano).

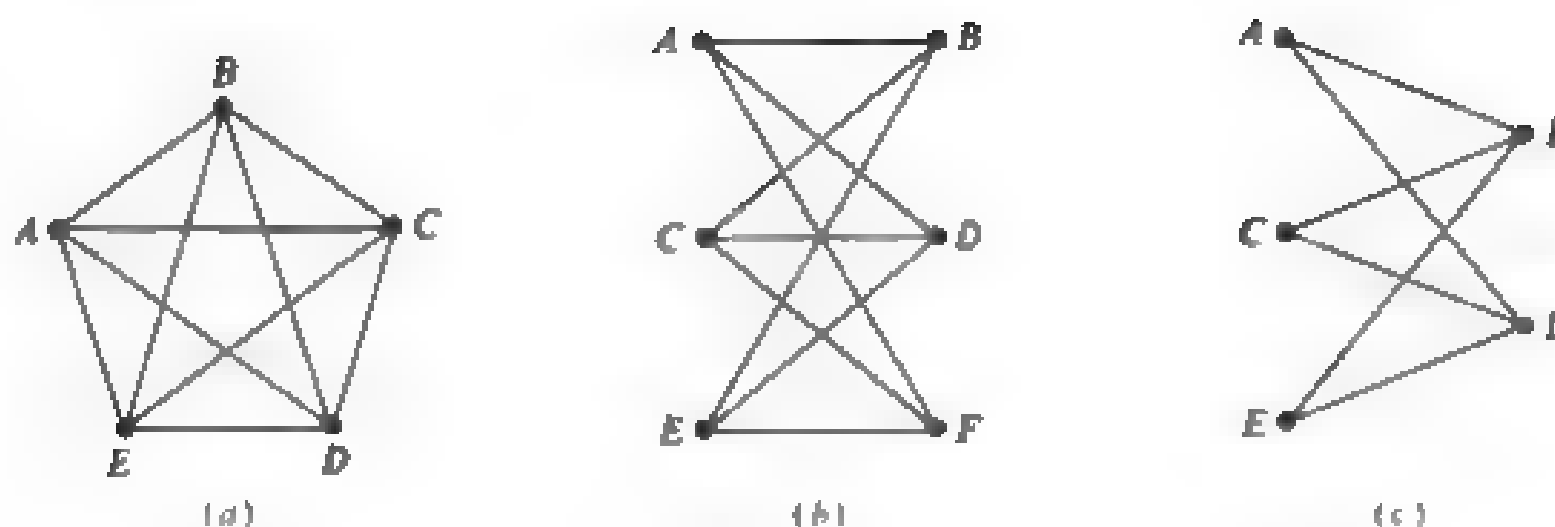



Figura 8-59

Grafos especiais

8.48 Desenhe dois grafos 3-regulares com: (a) oito vértices; (b) nove vértices.

8.49 Considere o grafo completo K_n.

(a) Encontre o diâmetro de K_n.

(b) Encontre o número m de arestas em K_n.

(c) Encontre o grau de cada vértice em K_n.

(d) Encontre os valores de n para os quais K_n é: (i) atravessável; (ii) regular.

8.50 Considere o grafo completo $K_{m,n}$.

(a) Encontre o diâmetro de $K_{m,n}$.

(b) Encontre o número E de arestas em $K_{m,n}$.

(c) Determine os $K_{m,n}$ que são atravessáveis.

(d) Quais dos grafos $K_{m,n}$ são isomorfos e quais são homeomorfos?

8.51 O n-cubo, denotado por $\mathbf{Q}_n$, é o grafo cujos vértices são os 2^n arrays de bits de comprimento n, e onde dois vértices são adjacentes se eles diferem em apenas uma posição. A Fig. 8-60(a) e (b) mostra os n-cubos $\mathbf{Q}_2$ e $\mathbf{Q}_3$.

(a) Encontre o diâmetro de $\mathbf{Q}_n$.

(b) Encontre o número m de arestas em $\mathbf{Q}_n$.

(c) Encontre o grau de cada vértice em $\mathbf{Q}_n$.

(d) Encontre os valores de n para os quais $\mathbf{Q}_n$ é atravessável.

(e) Encontre um circuito hamiltoniano (chamado de código de Gray) para (i) $\mathbf{Q}_3$, (ii) $\mathbf{Q}_4$.

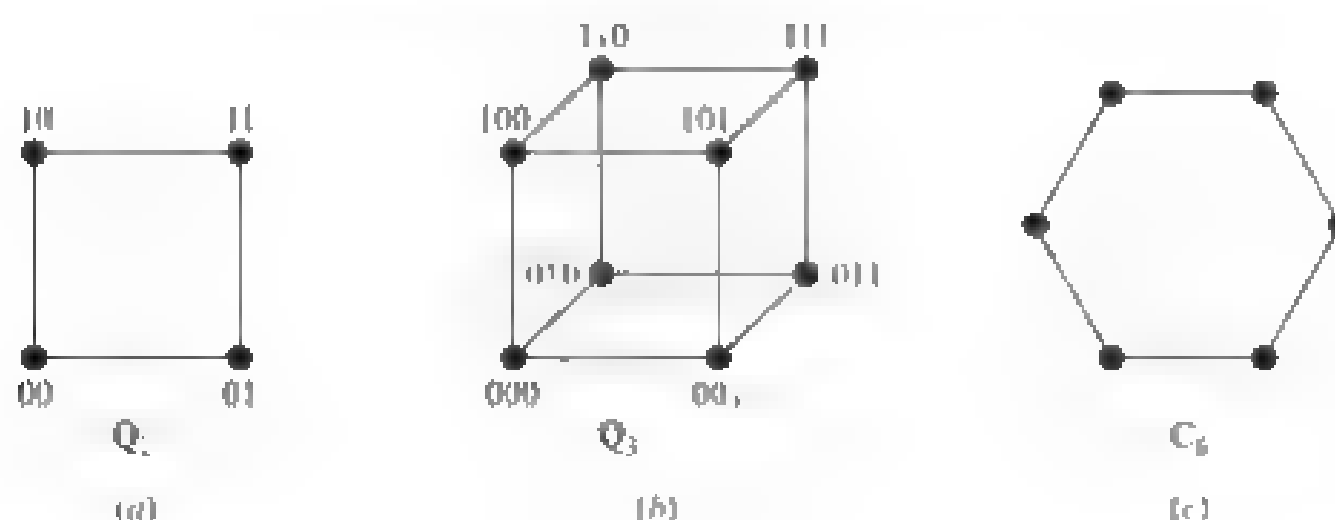



Figura 8-60

8.52 O n-ciclo, denotado por C_n, é o grafo que consiste em apenas um único ciclo de comprimento n. A Fig. 8-60(c) mostra o 6-ciclo C_6. (a) Encontre o número de vértices e arestas em C_n. (b) Encontre o diâmetro de C_n.

8.53 Descreva os grafos conexos que são bipartidos e regulares.

Árvores

8.54 Desenhe todas as árvores com cinco vértices ou menos.

8.55 Encontre o número de árvores com sete vértices.

8.56 Encontre o número de árvores geradoras na Fig. 8-61(*a*).

8.57 Encontre o peso de uma árvore geradora mínima na Fig. 8-61(*b*).

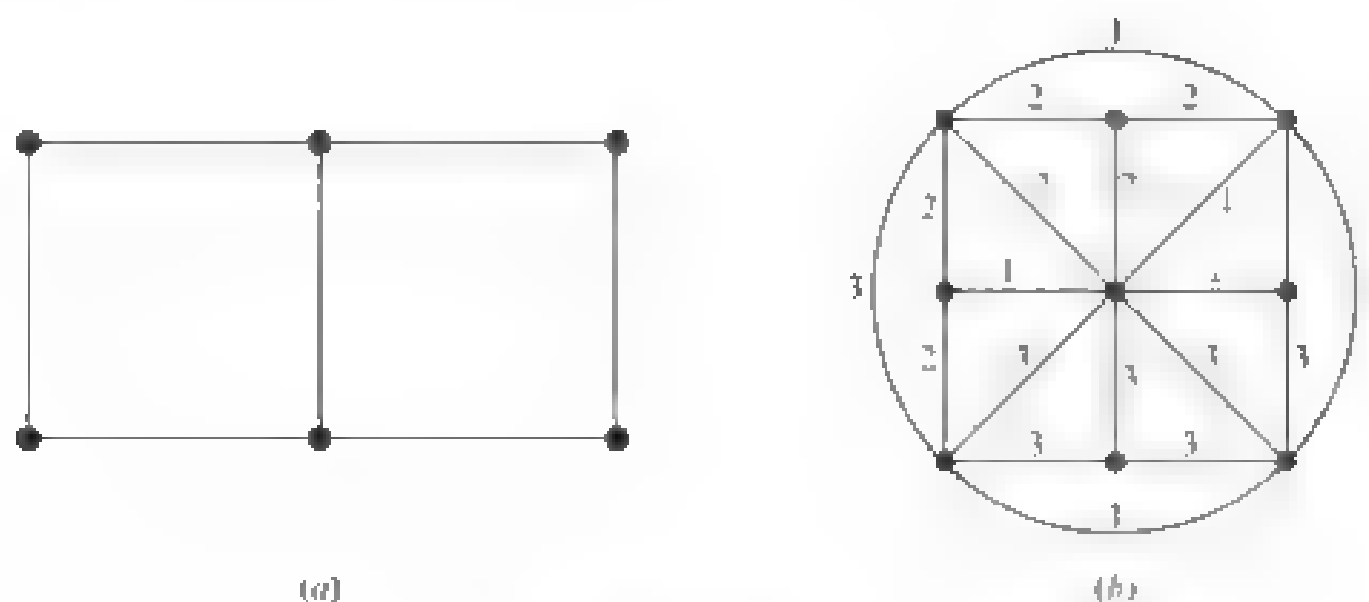



Figura 8-61

8.58 Mostre que qualquer árvore é um grafo bipartido.

8.59 Quais grafos bipartidos completos $K_{m,n}$ são árvores?

Grafos planares, mapas, coloração

8.60 Desenhe uma representação planar de cada grafo G na Fig. 8-62, se possível, caso contrário, mostre que tem um subgrafo homeomorfo a K_5 ou $K_{3,3}$.

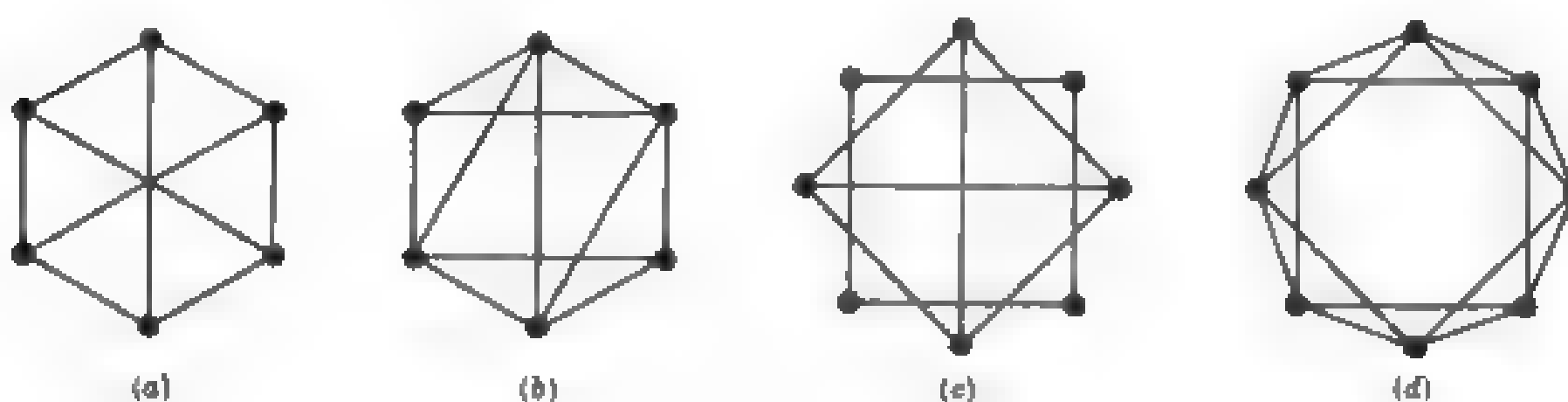



Figura 8-62

8.61 Mostre que o 3-cubo Q_3 (Fig. 8-60(*b*)) é planar

8.62 Para o mapa na Fig. 8-63, encontre o grau de cada região e verifique que a soma dos graus das regiões é igual ao dobro do número de arestas.

8.63 Conte o número V de vértices, o número E de arestas e o número R de regiões de cada um dos mapas na Fig. 8-64, e verifique a fórmula de Euler.

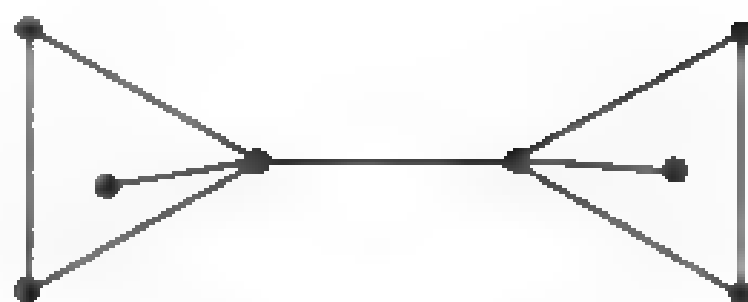



Figura 8-63

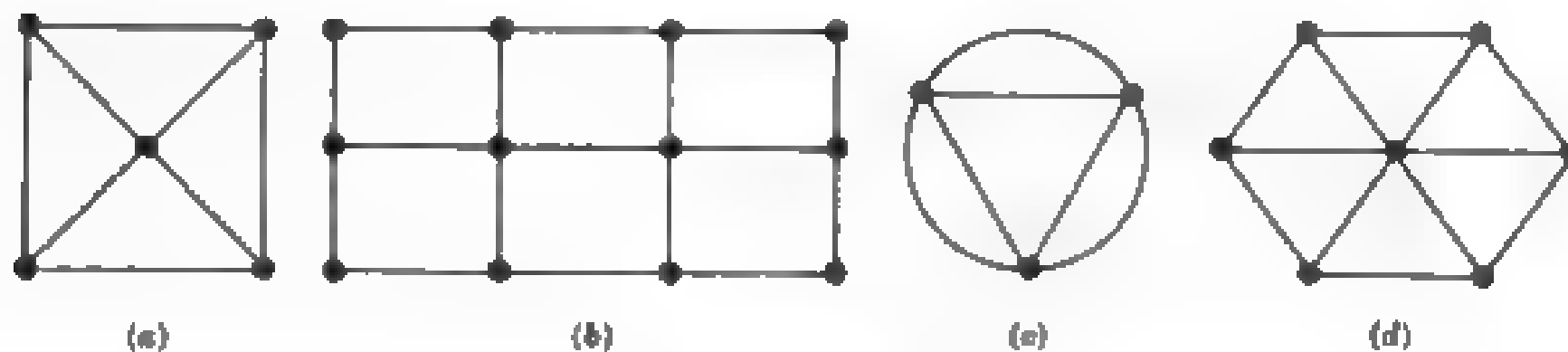



Figura 8-64

8.64 Encontre o número mínimo de cores necessárias para pintar as regiões de cada mapa na Fig. 8-64.

8.65 Desenhe o mapa que é dual a cada mapa na Fig. 8-64.

8.66 Use o algoritmo de Welch-Powell para pintar cada grafo na Fig. 8-65. Encontre o número cromático n do grafo.

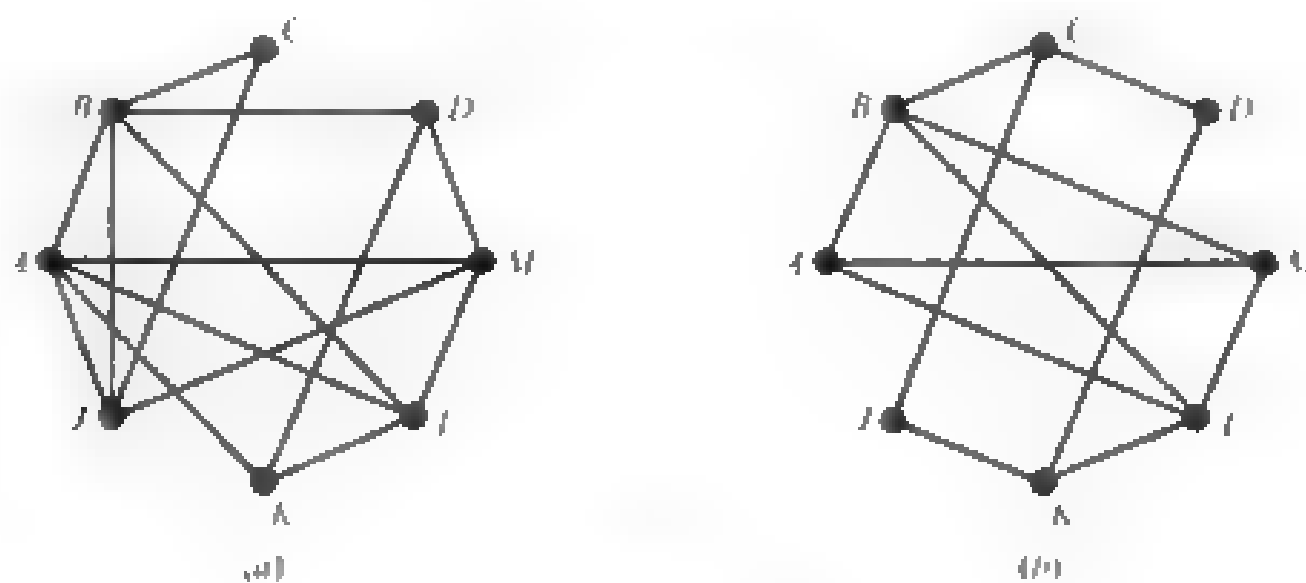



Figura 8-65

Representação sequencial de grafos

8.67 Encontre a matriz de adjacência A de cada multigrafo na Fig. 8-66.

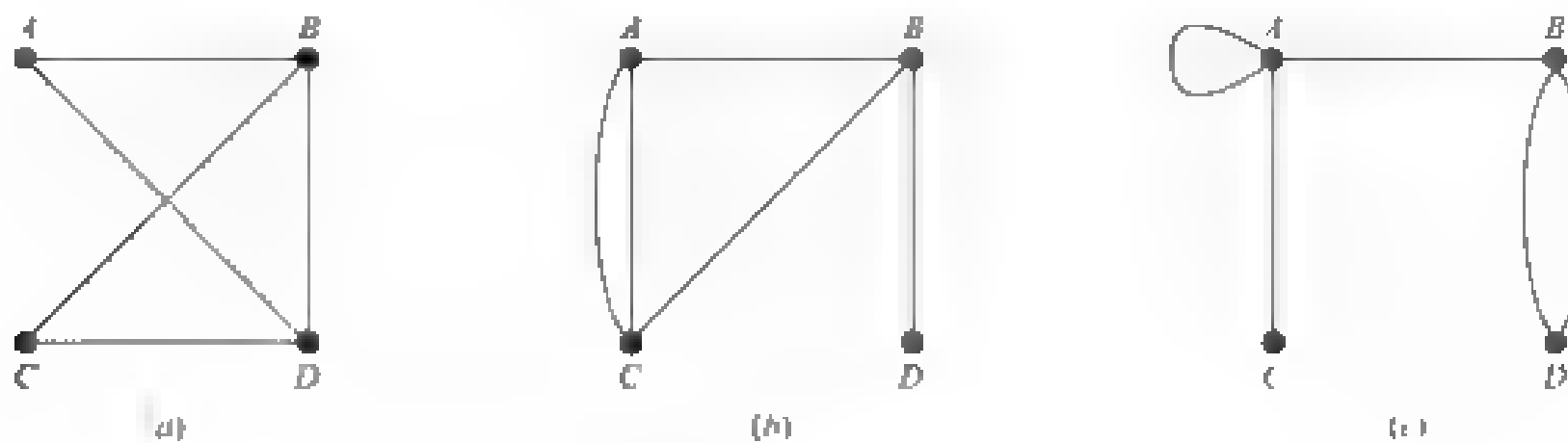



Figura 8-66

8.68 Esboce o multigrafo G correspondente a cada uma das seguintes matrizes de adjacência.

$$\text{(a) } A = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \qquad \text{(b) } A = \begin{bmatrix} & 1 & 1 & 2 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 2 & 0 & 2 & 2 \end{bmatrix}$$

8.69 Suponha que um grafo G é bipartido. Mostre que podemos ordenar os vértices de G, de modo que sua matriz de adjacência A tenha a forma $A = \begin{bmatrix} 0 & B \\ C & 0 \end{bmatrix}$

Representação ligada de grafos

8.70 Suponha que um grafo G seja armazenado na memória como na Fig. 8-67

Arquivo de vértices

START 7

	1	2	3	4	5	6	7	8
VERTEX	*C*		*F*	*E*	*A*		*B*	*D*
NEXT-V	0		5	1	8		3	4
PTR	2		11	6	12		4	1

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10	11	12
ADJ	7	7	4	5		7	1		8	3	1	7
NEXT	0	10	0	7		0	9		3	0	0	0

Figura 8-67

(a) Liste os vértices na ordem em que eles aparecem na memória.

(b) Encontre a estrutura de adjacência de G, ou seja, determine a lista de adjacência (v) de cada vértice v de G

8.71 Exiba a estrutura de adjacência (AS) para cada grafo G na Fig. 8-59.

8.72 A Fig. 8-68(*a*) mostra um grafo G representando seis cidades A, B, ..., F conectadas por sete rodovias numeradas 22, 33, ..., 88. Mostre como G pode ser mantido na memória, usando uma representação ligada com arrays específicos para as cidades e para as rodovias numeradas. (Observe que VERTEX é um array específico e, assim, o campo NEXT-V não é necessário.)

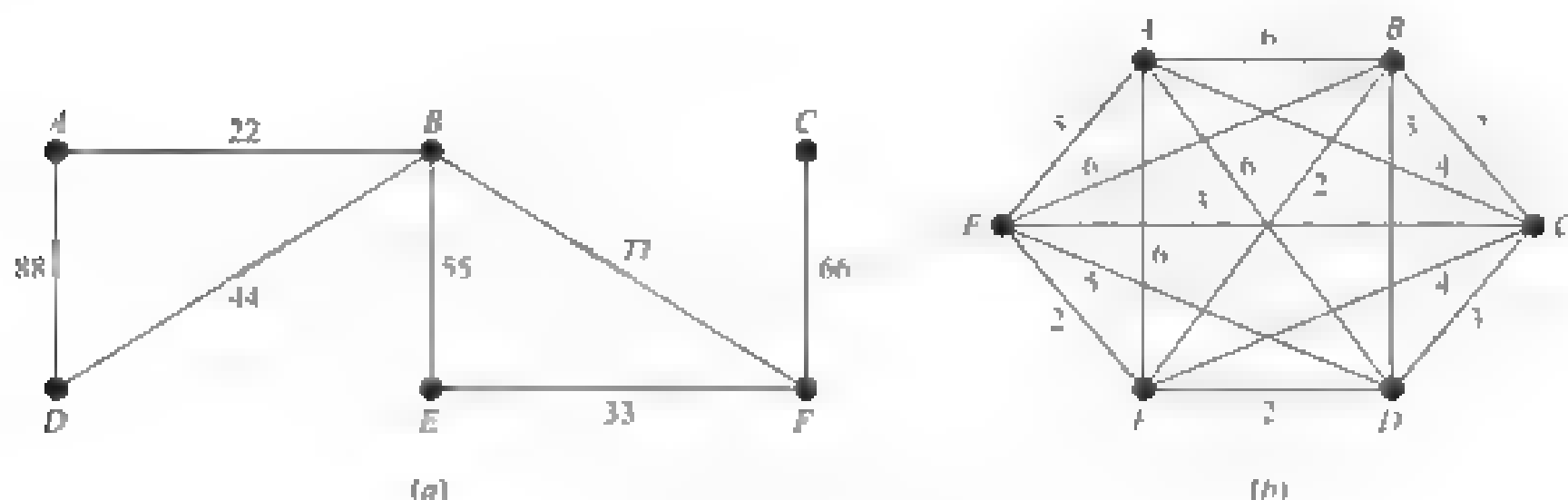



Figura 8-68

Problema do caixeiro viajante

8.73 Aplique o algoritmo do vizinho mais próximo no grafo ponderado completo G da Fig. 8-68(*b*), começando no (a) vértice A, (b) vértice B.

8.74 Considere o grafo ponderado completo G da Fig. 8-57 com cinco vértices.

(a) Começando no vértice A, liste os $H = (n - 1)!/2 = 12$ circuitos hamiltonianos de G e encontre o peso de cada um deles.

(b) Encontre um circuito hamiltoniano de peso mínimo.

Algoritmos de grafos

8.75 Considere o grafo G da Fig. 8-57 (onde os vértices são ordenados alfabeticamente).

(a) Encontre a estrutura de adjacência (AS) de G.

(b) Usando o Algoritmo DFS (busca em profundidade) 8.5 sobre G e iniciando no vértice C, encontre a sequência PILHA e a ordem na qual os vértices são processados.

(c) Repita (b) começando no vértice K.

8.76 Usando o Algoritmo BFS (busca em largura) 8.6 sobre o grafo G da Fig. 8-57, encontre a sequência FILA e a ordem na qual os vértices são processados, iniciando no: (a) vértice C; (b) vértice K.

8.77 Repita o Problema 8.75 para o grafo G na Fig. 8-65(a).

8.78 Repita o Problema 8.76 para o grafo G na Fig. 8-65(a).

8.79 Repita o Problema 8.75 para o grafo G na Fig. 8-65(b).

8.80 Repita o Problema 8.76 para o grafo G na Fig. 8-65(b).

Respostas dos Problemas Complementares

8.34 (a) 2, 4, 3, 2, 2, 2, 3, 2, (b) ABL, $ABKL$, $AJBL$, $AJBKL$, (c) BLC, $BKLC$, $BAJBLC$, $BAJBKLC$; (d) 3, (e) 4.

8.35 (a) $AJBA$, $BKLB$, $CDMC$; (b) B, C, L, (c) apenas $\{C, L\}$

8.36 $E' = \{BJ, BK, CD\}$; (b)$E' = \{AJ, CM, LC\}$; (c) $E' = \{BJ, DM\}$; (d) $E' = \{KL, LC, CM\}$. Além disso, (a) e (b) são isomorfos e (a), (b) e (c) são homeomorfos.

8.38 *Sugestão:* Considere um caminho simples maximal α e mostre que seus extremos têm grau 1.

8.40 Há cinco deles, como mostrado na Fig. 8-69.

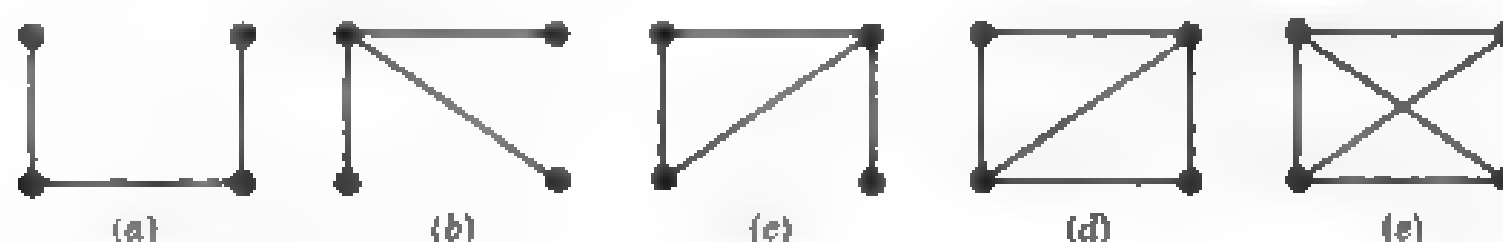



Figura 8-69

8.42 *Sugestão:* Use o Teorema 8.1.

8.43 Primeiro, delete todas as arestas de G que não estão em H e, em seguida, delete todos os vértices de G que não estão em H.

8.44 (a) Euleriano, pois todos os vértices são pares. $ABCDEACEBDA$. (b) Nenhum dos casos, uma vez que quatro vértices são ímpares. (c) Caminho euleriano começando em B e terminando em D (ou vice-versa). $BADCBED$.

8.45 (a) $ABCDEA$, (b) $ABCDEFA$, (c) nenhum dos casos, pois B ou D deve ser visitado duas vezes em qualquer caminho fechado, incluindo todos os vértices.

8.46 $(5 - 1)!/2 = 12$.

8.47 *Sugestão*: Adicionando um vértice pela divisão de uma aresta, não muda o grau dos vértices originais e simplesmente acrescenta um vértice de grau par.

8.48 (a) Os dois grafos 3-regulares da Fig. 8-70 não são isomorfos: (b) tem um 5-ciclo, mas (a) não tem. (b) Não existe. A soma dos graus de um grafo r-regular com s vértices é rs, e rs deve ser par.

(a)

(b)

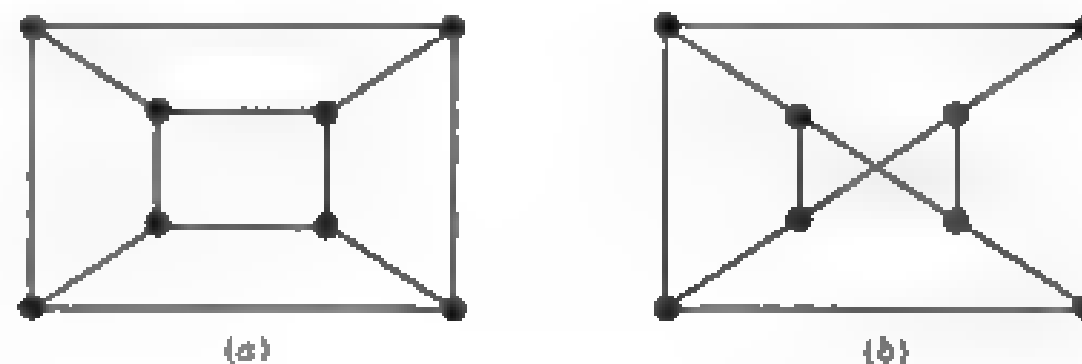



Figura 8-70

8.49 (a) $\text{diam}(K_1) = 0$; todos os demais têm diâmetro 1, (b) $m = C(n, 2) = n(n-1)/2$, (c) $n - 1$, (d) (i) $n = 2$ e n ímpar; (ii) todos os n.

8.50 (a) $\text{diam}(K_{1,1}) = 1$, todos os demais têm diâmetro 2, (b) $E = mn$, (c) $K_{1,1}$, $K_{1,2}$ e $K_{m,n}$, onde m e n são pares, (d) não há isomorfos, apenas $K_{1,1}$ e $K_{1,2}$ são homeomorfos.

8.51 (a) n; (b) $n2^{n-1}$; (c) n; (d) $n = 1$, par; (e) considere a matriz 4×16.

$$M = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

que mostra como Q_4 (as colunas de M) é obtido a partir de Q_3. Ou seja, a submatriz superior à esquerda 3×8 de M é Q_3, a superior à direita 3×8 de M é Q_3, escrita ao contrário, e a última linha consiste em oito 0's seguidos de oito 1's.

8.52 (a) n e n; (b) $n/2$ quando n é par, $(n + 1)/2$ quando n é ímpar.

8.53 $K_{m,n}$ é bipartido e m-regular. Além disso, começando com $K_{m,n}$, delete m arestas disjuntas para obter um grafo bipartido que seja $(m - 1)$-regular, delete outras m arestas disjuntas para obter um grafo bipartido que seja $(m - 2)$-regular, e assim por diante. Esses grafos podem ser desconexos, mas suas componentes conexas têm as propriedades desejadas.

8.54 Há oito dessas árvores, como mostrado na Fig. 8-71. O grafo com um vértice e sem arestas é chamado de *árvore trivial*.

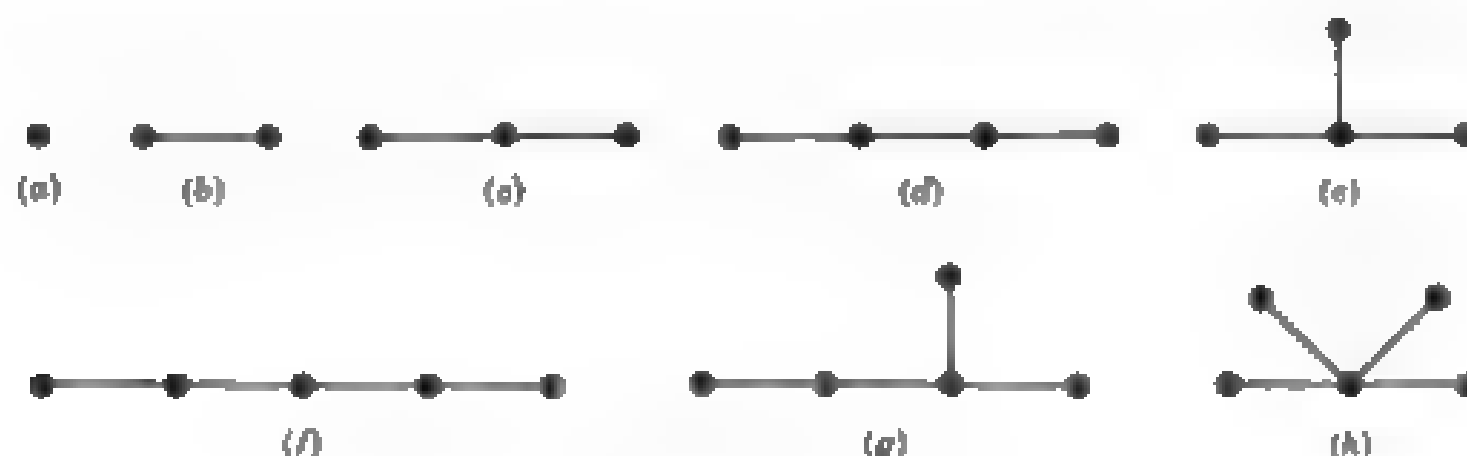



Figura 8-71

8.55 10

8.56 15

8.57 $1 + 1 + 1 + 1 + 1 + 2 + 2 + 3 = 12$

8.59 $m = 1$

8.60 Apenas (a) é não planar, e $K_{3,3}$ é um subgrafo.

8.61 A Fig. 8-70(*a*) é uma representação planar de Q_3.

8.62 A região externa tem grau 8 e as outras duas regiões têm grau 5.

8.63 (a) 5, 8, 5, (b) 12, 17, 7; (c) 3, 6, 5; (d) 7, 12, 7

8.64 (a) 3; (b) 3; (c) 2, (d) 3.

8.65 Ver Fig. 8-72.

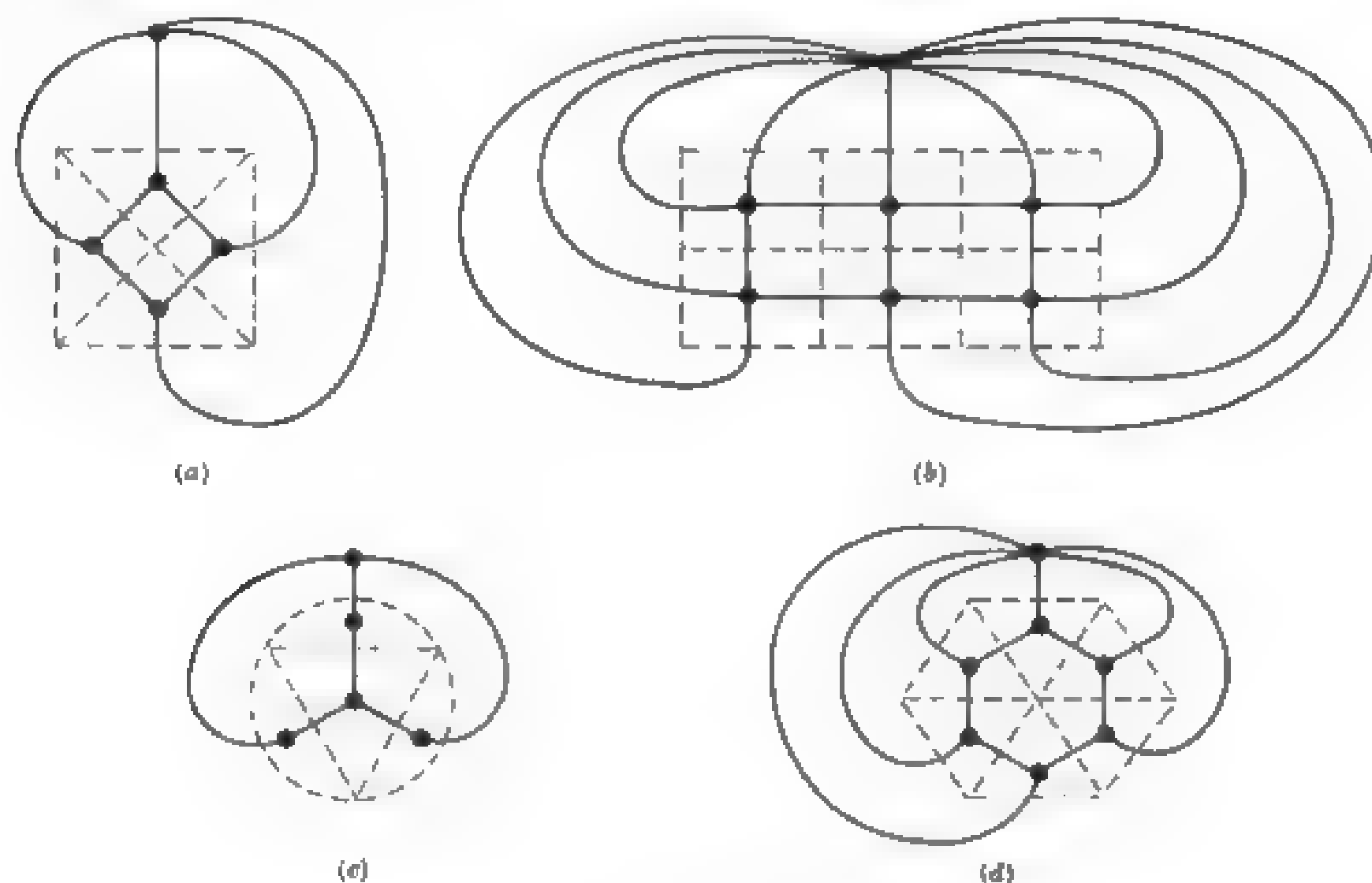



Figura 8-72

8.66 (a) $n = 3$, (b) $n = 4$.

8.67 (*a*) $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ (*b*) $\begin{bmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{bmatrix}$

8.68 Ver Fig. 8-73.

8.69 Sejam *M* e *N* dois conjuntos disjuntos de vértices determinando o grafo bipartido *G*. Ordene primeiro os vértices de *M* e depois os de *N*.

8.70 (a) *B, F, A, D, E, C.*

(b) $G = [A{:}B;\ B{:}A, C, D, E;\ C{:}F;\ D{:}B;\ E{:}B;\ F{:}C]$

(a) (b)

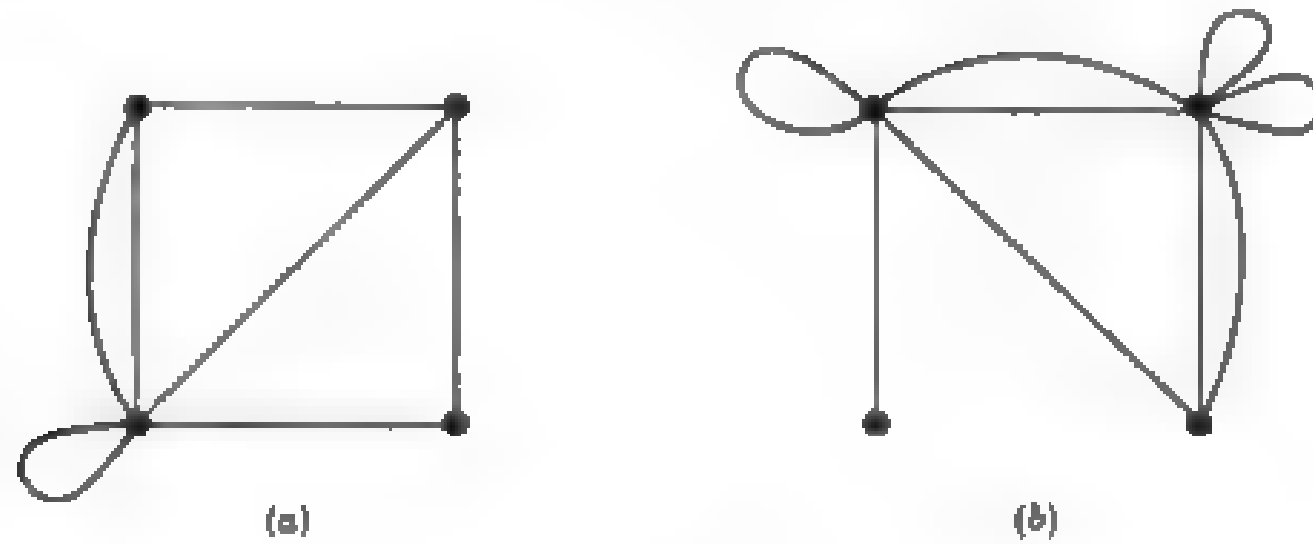



Figura 8-73

8.71 (a) Cada vértice é adjacente aos outros quatro.

(b) $G = [A{:}B, D, F;\ B{:}A, C, E;\ C{:}B, D, F;\ D{:}A, C, E;\ E{:}B, D, F;\ F{:}A, C, E]$

(c) $G = [A{:}B, D;\ B{:}A, C, E;\ C{:}B, D;\ D{:}A, C, E;\ E{:}B, D]$

8.72 Ver Fig. 8-74.

Arquivo de vértices

	1	2	3	4	5	6	7	8
VÉRTICE	*A*	*B*	*C*	*D*	*E*	*F*		
PTR		2	9	14	8	12		

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
NÚMERO	22	22	33	33	44	44	55	55	66	66	77	77	88	88	
ADJ	2	1	6	5	4	2	5	2	6	3	6	2	4		
NEXT	13	5	0	0	7	0	11	3	0	4	0	10	0	6	

Figura 8-74

8.73 (a) $|ACBEDFA| = 20$ ou $|ACBEFDA| = 21$. (b) $|BCFEDAB| = 21$ ou $|BCDEFAB| = 20$

8.74 (a) $|ABCDEA| = 775$, $|ABCEDA| = 725$, $|ABDCEA| = 1100$, $|ABDECA| = 900$, $|ABECDA| = 1050$, $|ABEDCA| = 900$, $|ACBDEA| = 825$, $|ACBEDA| = 775$, $|ACDBEA| = 1150$, $|ACEBDA| = 1100$, $|ADBCEA| = 975$, $|ADCBEA| = 975$

(b) $|ABCEDA| = 725$

8.75 (a) $G = [A{:}BJ;\ B{:}AJKL;\ C{:}DLM;\ D{:}CM;\ J{:}AB;\ K{:}BL;\ L{:}BCK;\ M{:}CD]$

(b) [PILHA: *C, MLD, DL, L, KB, B, J, A*], *CMDLKBJA*

(c) [PILHA: *K, LB, CB, MDB, DB, B, JA, A*], *KLCMDBJA*

8.76 (a) [FILA: *C, MLD, ML, L, KB, JAK, JA, J*], *CDMLBKAJ*

(b) [FILA: *K, LB, JAL, CJA, CJ, C, MD, M*], *KBLAJCDM*

8.77 (a) $G = [A{:}BMJKL;\ B{:}ACDJL;\ C{:}BJ;\ D{:}BKM;\ J{:}ABCM;\ K{:}ADL;\ L{:}ABKM;\ M{:}ADJL]$

(b) [PILHA: *C, JB, MBA, LDAB, KBAD, DAB, AB, B*], *CJMLKDAB*

(c) [PILHA: *K, LDA, MBAD, JDAB, CBAD, BAD, AD, D*], *KLMJCBAD*

8.78 (a) [FILA: *C*, *JB*, *LDAJ*, *MLDA*, *KMLD*, *KML*, *KM*, *K*], *CBJADLMK*

(b) [FILA: *K*, *LDA*, *JMBLD*, *JMBL*, *CJMB*, *CJM*, *CJ*, *C*], *KADLBMJC*

8.79 (a) $G = [A{:}BLM;\ B{:}ACLM;\ C{:}BDJ;\ D{:}CK;\ J{:}CK;\ K{:}DJL;\ L{:}ABKM;\ M{:}ABL]$

(b) [PILHA : *C*, *JDB*, *KDB*, *LDB*, *MBAD*, *BAD*, *AD*, *D*], *CJKLMBAD*

(c) [PILHA : *K*, *LJD*, *MBAJD*, *BAJD*, *CAJD*, *JDA*, *DA*, *A*], *KLMBCJDA*

8.80 (a) [FILA: *C*, *JDB*, *MLAJD*, *KMLAJ*, *KMLA*, *KML*, *KM*, *K*], *CBDJALMK*

(b) [FILA : *K*, *LJD*, *CLJ*, *CL*, *MBAC*, *MBA*, *MB*, *M*], *KDJLCABM*

Grafos Orientados

9.1 INTRODUÇÃO

Grafos orientados são grafos nos quais as arestas são em um sentido. Tais grafos são frequentemente mais úteis em vários sistemas dinâmicos, como computadores e sistemas de fluxo. Contudo, essa característica extra torna mais difícil determinar certas propriedades sobre o grafo. Isto é, processar esses grafos pode ser semelhante a viajar em uma cidade por muitas ruas de sentido único.

Este capítulo nos dá as definições básicas e propriedades de grafos orientados. Muitas das definições são semelhantes àquelas do capítulo anterior sobre grafos (não orientados). Contudo, por motivos pedagógicos, este capítulo é, em grande parte, independente do anterior.

9.2 GRAFOS ORIENTADOS

Um *grafo orientado G* ou *dígrafo* (ou, simplesmente, grafo) consiste em duas coisas:

(i) Um conjunto V cujos elementos são chamados de *vértices*, *nós* ou *pontos*.

(ii) Um conjunto E de pares *ordenados* (u, v) de vértices chamados de *arcos* ou *arestas orientadas* ou, simplesmente, *arestas*.

Escrevemos $G(V, E)$ quando queremos enfatizar as duas partes de G. Também escrevemos $V(G)$ e $E(G)$ para denotar, respectivamente, os conjuntos de vértices e de arestas de um grafo G. (Se não for explicitamente estabelecido, o contexto usualmente determina se um grafo G é ou não orientado.)

Suponha que $e = (u, v)$ é uma aresta orientada em um grafo G. Então a terminologia a seguir é empregada.

(a) e *começa* em u e *termina* em v.

(b) u é a *origem* ou *ponto inicial* de e, e v é o *destino* ou *ponto terminal* de e.

(c) v é um *sucessor* de u.

(d) u *é adjacente a* v, e v *é adjacente de* u.

Se $u = v$, então e é chamado de *laço*.

O conjunto de todos os sucessores de um vértice u é importante; ele é denotado e formalmente definido como

$$\text{succ}(u) = \{v \in V \mid \text{existe uma aresta } (u, v) \in E\}$$

Esse conjunto é chamado de *lista de sucessores* ou *lista de adjacência* de u.

Uma *imagem* de um grafo orientado G é uma representação de G no plano. Ou seja, cada vértice u de G é representado por um ponto (ou um pequeno círculo), e cada aresta (orientada) $e = (u, v)$ é representada por uma flecha ou curva orientada do ponto inicial u de e ao ponto terminal v. Geralmente se apresenta um grafo orientado G por sua imagem em vez de uma lista explícita de seus vértices e arestas.

Se as arestas e/ou vértices de um grafo orientado G são rotulados com algum conjunto de dados, então G é chamado de *grafo orientado rotulado.*

Um grafo orientado (V, E) é dito *finito* se seus conjuntos de vértices V e arestas E forem finitos.

Exemplo 9.1

(a) Considere o grafo orientado G representado na Fig. 9-1(a). Ele consiste em quatro vértices A, B, C e D, ou seja, $V(G) = \{A, B, C, D\}$, e nas sete arestas a seguir:

$$E(G) = \{e_1, e_2, \ldots, e_7\} = \{(A, D), (B, A), (B, A), (D, B), (B, C), (D, C), (B, B)\}$$

As arestas e_2 e e_3 são ditas *paralelas*, uma vez que ambas começam em B e terminam em A. A aresta e_7 é um *laço*, pois começa e termina em B.

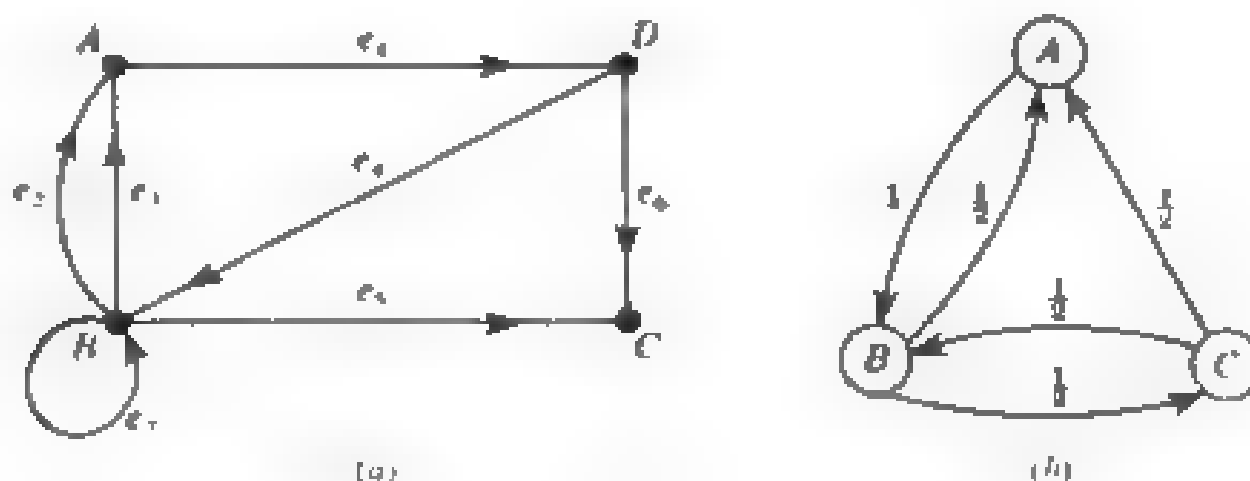



Figura 9-1

(b) Suponha que três garotos, A, B e C, estão jogando uma bola, um para o outro, de modo que A sempre joga a bola para B, mas B e C podem jogar tanto para A quanto um para o outro. Esse sistema dinâmico é retratado na Fig. 9-1(b), onde arestas são rotuladas com as respectivas probabilidades, ou seja, A joga a bola para B com probabilidade 1, B joga a bola para A e C, ambos com probabilidade 1/2, e C joga a bola para A e B, cada um com probabilidade 1/2.

Subgrafos

Sejam $G = G(V, E)$ um grafo orientado e V' um subconjunto do conjunto V de vértices de G. Suponha que E' é um subconjunto de E tal que os pontos extremos das arestas de E' pertencem a V'. Então, $H(V', E')$ é um grafo orientado e é chamado de *subgrafo* de G. Especificamente, se E' contém todas as arestas de E cujos pontos extremos pertencem a V', então $H(V', E')$ é dito o subgrafo de *gerado* ou *determinado* por V'. Por exemplo, para o grafo $G = G(V, E)$ na Fig. 9-1(a), $H(V', E')$ é o subgrafo de G determinado pelo conjunto de vértices V', onde

$$V' = \{B, C, D\} \text{ e } E' = \{e_4, e_5, e_6, e_7\} = \{(D, B), (B, C), (D, C), (B, B)\}$$

9.3 DEFINIÇÕES BÁSICAS

Esta seção discute as questões de graus de vértices, caminhos e conectividade em um grafo orientado.

Graus

Suponha que G é um grafo orientado. O *grau de saída* de um vértice v de G, denotado por outdeg(v), é o número de arestas começando em v, e o *grau de entrada* de v, denotado por indeg(v), é o número de arestas terminando em v. Como cada aresta começa e termina em um vértice, imediatamente obtemos o seguinte teorema.

Teorema 9.1: A soma dos graus de saída dos vértices de um grafo orientado G é igual à soma dos graus de entrada dos vértices, que é igual ao número de arestas de G.

O vértice v com grau de entrada zero é chamado de *fonte*, e um vértice v com grau de saída zero é dito um *poço*.

Exemplo 9.2 Considere o grafo G na Fig. 9-1(a). Temos

$$\text{outdeg}(A) = 1, \quad \text{outdeg}(B) = 4, \quad \text{outdeg}(C) = 0, \quad \text{outdeg}(D) = 2,$$
$$\text{indeg}(A) = 2, \quad \text{indeg}(B) = 2, \quad \text{indeg}(C) = 2, \quad \text{indeg}(D) = 1.$$

Como esperado, a soma dos graus de saída é igual à soma dos graus de entrada, que é igual ao número 7 de arestas. O vértice C é um poço, pois nenhuma aresta começa em C. O grafo não tem fontes.

Caminhos

Seja G um grafo orientado. Os conceitos de caminho, caminho simples, trilha e ciclo podem ser aplicados de grafos não orientados para o grafo orientado G, exceto o de direções das arestas, que deve concordar com a direção do caminho. Especificamente:

(i) Um *caminho (orientado)* P em G é uma sequência alternada de vértices e arestas orientadas, digamos,

$$P = (v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n)$$

tal que cada aresta e_i começa em v_{i-1} e termina em v_i. Se não há ambiguidade, denotamos P por sua sequência de vértices ou sua sequência de arestas.

(ii) O *comprimento* do caminho P é n, seu número de arestas.

(iii) Um *caminho simples* é um caminho com vértices distintos. Uma *trilha* é um caminho com arestas distintas.

(iv) Um *caminho fechado* tem os mesmos vértices inicial e terminal.

(v) Um *caminho gerador* contém todos os vértices de G.

(vi) Um *ciclo* (ou *circuito*) é um caminho fechado com vértices distintos (exceto o primeiro e o último).

(vii) Um *semicaminho* é o mesmo que um caminho, exceto que a aresta e_i pode começar em v_{i-1} ou v_i e terminar no outro vértice. *Semitrilhas* e *caminhos semissimples* são definidos de forma análoga.

Um vértice v é *alcançável* a partir de um vértice u se existir um caminho de u a v. Se v é alcançável a partir de u, então (por eliminação de arestas redundantes) deve haver um caminho simples de u a v.

Exemplo 9.3 Considere o grafo G na Fig. 9-1(a).

(a) A sequência $P_1 = (D, C, B, A)$ é um semicaminho, mas não um caminho, uma vez que (C, B) não é uma aresta, isto é, a direção de $e_5 = (C, B)$ não concorda com a direção de P_1.

(b) A sequência $P_2 = (D, B, A)$ é um caminho de D a A, pois (D, B) e (B, A) são arestas. Logo, A é alcançável a partir de D.

Conectividade

Existem três tipos de conectividade em um grafo orientado G.

(i) G é *fortemente conexo* ou *forte* se, para qualquer par de vértices u e v de G, há um caminho de u a v e um caminho de v a u, isto é, cada um é alcançável a partir do outro.

(ii) G é *unilateralmente conexo* ou *unilateral* se, para qualquer par de vértices u e v de G, existe um caminho de u a v ou um caminho de v a u; ou seja, um deles é alcançável a partir do outro.

(iii) G é *fracamente conexo* ou *fraco* se, existe um semicaminho entre qualquer par de vértices u e v em G

Seja G' o grafo (não orientado) obtido de um grafo orientado G, permitindo que todas as arestas de G sejam não orientadas. Fica claro que G é fracamente conexo se, e somente se, o grafo G' é conexo.

Observe que conectividade forte implica conectividade unilateral, a qual implica conectividade fraca. Dizemos que G é estritamente unilateral se for unilateral, mas não fortemente conexo. E dizemos que G é estritamente fraco se for fraco, mas não unilateral.

Conectividade pode ser caracterizada em termos de caminhos geradores como se segue:

Teorema 9.2: Seja G um grafo orientado finito. Então:

(i) G é forte se, e somente se, G tem um caminho gerador fechado.

(ii) G é unilateral se, e somente se, G tem um caminho gerador

(iii) G é fraco se, e somente se, G tem semicaminho gerador.

Exemplo 9.4 Considere o grafo G na Fig. 9-1(a). Ele é fracamente conexo, uma vez que o grafo não orientado subjacente é conexo. Não há caminho de C para qualquer outro vértice, isto é, C é um poço e, assim, G não é fortemente conexo. Contudo, $P = (B, A, D, C)$ é um caminho gerador e, assim, G é unilateralmente conexo.

Grafos com fontes e poços aparecem em muitas aplicações (como diagramas de fluxo e redes). Uma condição suficiente para tais vértices existirem é a que se segue:

Teorema 9.3: Suponha que um grafo orientado finito G seja livre de ciclos, ou seja, não contém ciclos (orientados). Então G contém uma fonte e um poço.

Demonstração: Seja $P = (v_0, v_1, \ldots, v_n)$ um caminho simples de comprimento máximo, que existe, uma vez que G é finito. Então, o último vértice v_n é um poço; caso contrário, uma aresta (v_n, u) deve estender P ou formar um ciclo de $u = v_i$, para algum i. Analogamente, o primeiro vértice v_0 é uma fonte.

9.4 ÁRVORES ENRAIZADAS

Lembre que uma árvore é um grafo livre de ciclos e conexo, ou seja, um grafo conexo sem quaisquer ciclos. Uma *árvore enraizada* é uma árvore com um vértice designado r, chamado de *raiz* da árvore. Como existe um único caminho simples da raiz a qualquer outro vértice v de T, isso determina uma direção para as arestas de T. Assim, T deve ser vista como um grafo orientado. Observamos que qualquer árvore pode ser transformada em uma árvore enraizada simplesmente selecionando um dos vértices como a raiz.

Considere uma árvore enraizada T cuja raiz é r. O comprimento do caminho da raiz r a qualquer vértice v é chamado de *nível* (ou *profundidade*) de v, e o nível máximo é dito a *profundidade* ou *altura* da árvore. Os vértices de grau 1, que não sejam a raiz r, são chamados de *folhas* de T, e um caminho orientado de um vértice para uma folha é chamado de *ramo*.

Geralmente se desenha uma imagem de uma árvore enraizada, colocando a raiz no topo da árvore. A Fig. 9-2(a) mostra uma árvore T com raiz r e 10 outros vértices. A árvore tem cinco folhas, d, f, h, i e j. Observe que: *nível*(a) = 1, *nível*(f) = 2, *nível*(j) = 3. Além disso, a altura da árvore é 3.

O fato de que uma árvore enraizada T fornece uma direção para as arestas significa que podemos apresentar uma relação de precedência entre os vértices. Especificamente, dizemos que um vértice u *precede* um vértice v ou que v *segue* u, se existe um caminho (orientado) de v a u. Em particular, dizemos que v *segue imediatamente* u se (u, v) é uma aresta, ou seja, se v segue u e v é adjacente a u. Observamos que todo vértice v, exceto a raiz, segue imediatamente um único vértice, mas que v pode ser imediatamente seguido por mais de um vértice. Por

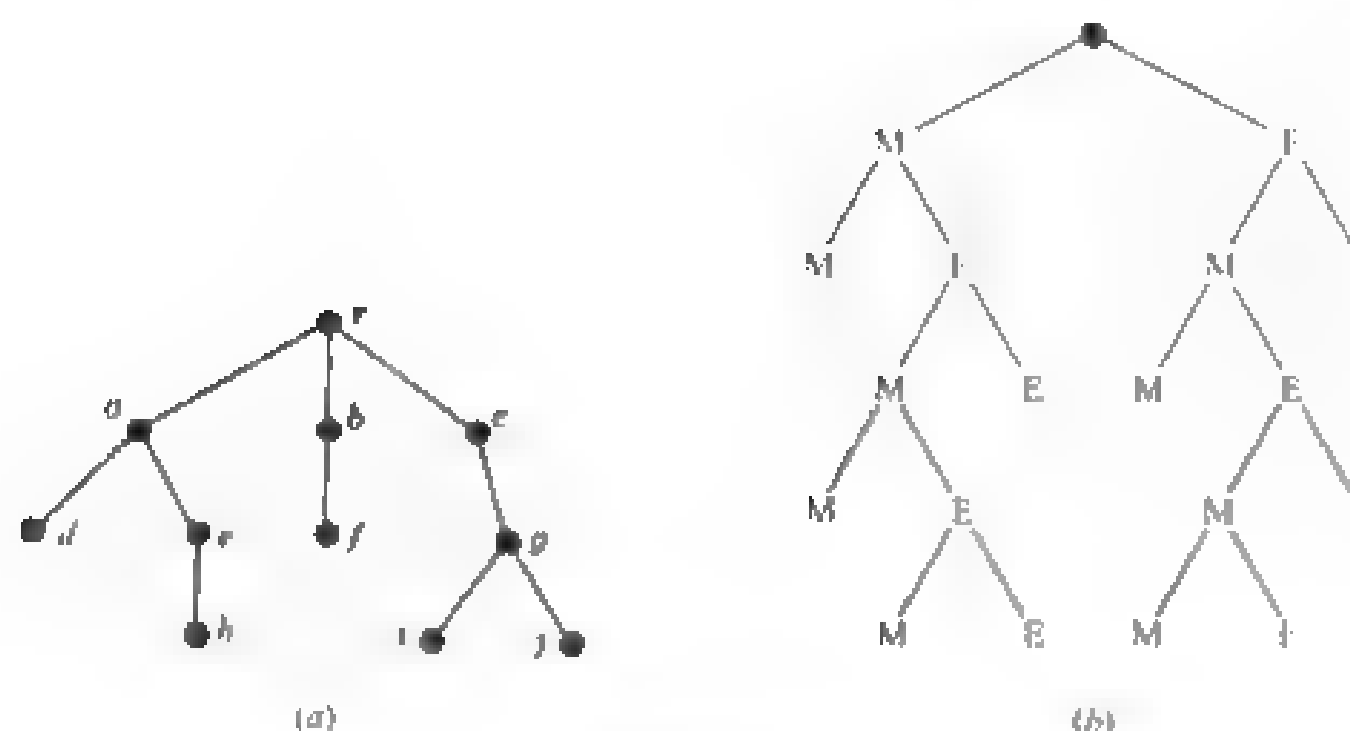



Figura 9-2

exemplo, na Fig. 9-2(a), o vértice j segue c, mas segue imediatamente g. Além disso, ambos i e j seguem imediatamente g.

Uma árvore enraizada T é também um instrumento útil para enumerar todas as possibilidades lógicas de uma sequência de eventos, onde cada evento pode ocorrer em uma quantia finita de maneiras. Isso é ilustrado no seguinte exemplo.

Exemplo 9.5 Suponha que Marcos e Érico estão disputando um torneio de tênis, de modo que o primeiro a vencer dois jogos seguidos, ou ganhar um total de três partidas, vence o torneio. Encontre o número de maneiras que o torneio pode ocorrer.

A árvore enraizada da Fig. 9-2(b) mostra as várias maneiras como o torneio pode decorrer. Há 10 folhas que correspondem às 10 maneiras que o torneio pode transcorrer.

MM, MEMM, MEMEM, MEMEE, MEE, EMM, EMEMM, EMEME, EMEE, EE

Especificamente, o caminho da raiz à folha descreve quem venceu quais jogos em tal torneio.

Árvores ordenadas enraizadas

Considere uma árvore enraizada T na qual as arestas saindo de cada vértice são ordenadas. Então temos os conceito de uma *árvore ordenada enraizada*. É possível sistematicamente rotular (ou *nomear*) os vértices dessa árvore como se segue. Primeiro, assinalamos 0 para a raiz r. A seguir, assinalamos 1, 2, 3, . . . aos vértices que imediatamente seguem r à medida que as arestas são ordenadas. Então rotulamos os demais vértices da seguinte maneira. Se a é o rótulo de um vértice v, então $a.1$, $a.2$, . . . são assinalados aos vértices que imediatamente seguem v à medida que as arestas são ordenadas. Ilustramos esse sistema de nomeação na Fig. 9-3(a), onde arestas são retratadas da esquerda para a direita de acordo com sua ordem. Observe que o número de pontos decimais em qualquer rótulo é um a menos do que o nível do vértice. Referimo-nos a esse sistema de nomeação como *sistema universal* para uma árvore ordenada enraizada.

O sistema universal de nomeação nos dá uma maneira importante para descrever (ou armazenar) linearmente uma árvore ordenada enraizada. Especificamente, dados os nomes a e b, fazemos $a < b$ se $b = a.c$, (ou seja, a é um *segmento inicial* de b), ou se existem inteiros positivos m e n com $m < n$ tais que

$$a = r.m.s \quad \text{e} \quad b = r.n.t$$

Essa ordem é chamada de *ordem lexicográfica*, pois é semelhante à maneira como as palavras são arranjadas em um dicionário. Por exemplo, os nomes na Fig. 9-3(a) são linearmente ordenados como representado na Fig. 9-3(b).

Essa ordem lexicográfica é idêntica à ordem obtida, deslocando para baixo o ramo mais à esquerda da árvore, depois, o próximo ramo à direita, seguido do segundo ramo à direita, e assim por diante.

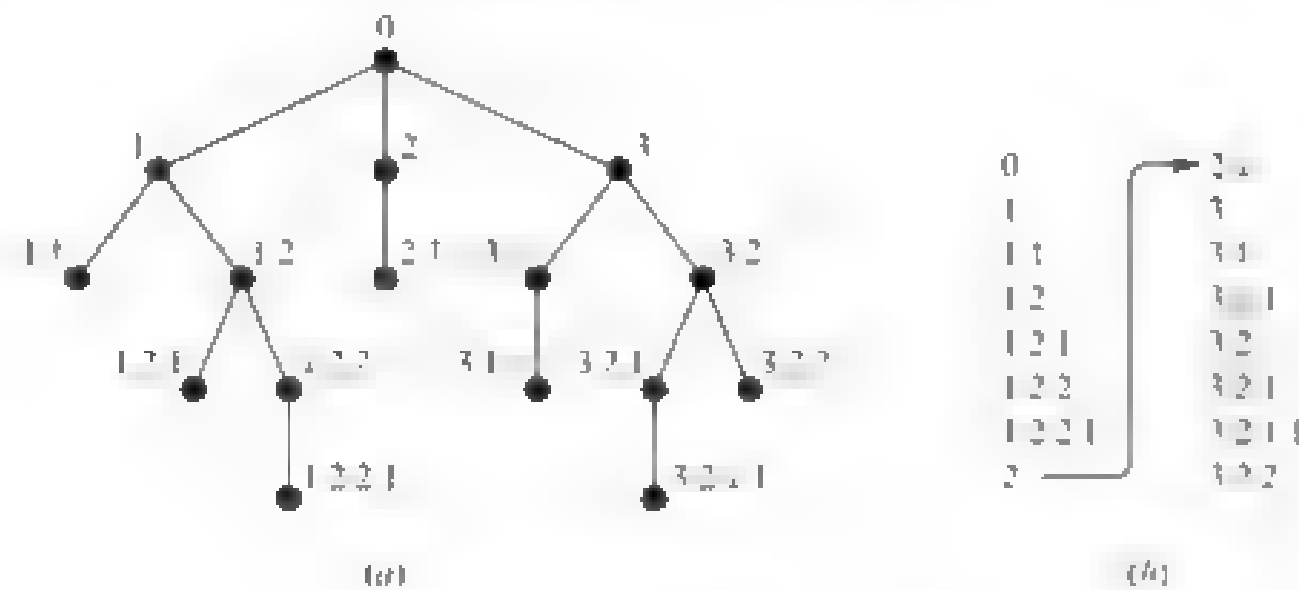



Figura 9-3

9.5 REPRESENTAÇÃO SEQUENCIAL DE GRAFOS ORIENTADOS

Existem duas maneiras principais de manter um grafo orientado G na memória de um computador. Uma delas, conhecida como a *representação sequencial* de G, é por meio de sua matriz de adjacência A. A outra maneira, chamada de *representação ligada* de G, é por meio de listas ligadas de vizinhos. Esta seção cobre a primeira representação. A representação ligada é discutida na Seção 9.7.

Suponha que um grafo G tem m vértices (nós) e n arestas. Dizemos que G é *denso* se $m = O(n^2)$ e *esparso* se $m = O(n)$ ou mesmo se $m = O(n \log n)$. A representação matricial de G é geralmente usada quando G é denso, e listas ligadas são usualmente empregadas quando G é esparso. Independentemente da maneira como se mantém um grafo G na memória, o grafo G é em geral inserido no computador pela sua definição formal, isto é, como uma coleção de vértices e uma coleção de arestas (pares de vértices).

Observação: Para evitar casos especiais de nossos resultados, assumimos, a menos que seja dito o contrário, que $m > 1$, onde m é o número de vértices de nosso grafo G. Portanto, G não é conexo se G não tem arestas.

Grafos orientados e relações, matriz de adjacência

Seja $G(V, E)$ um grafo orientado *simples*, isto é, um grafo sem arestas paralelas. Então, E é simplesmente um subconjunto de $V \times V$ e, portanto, E é uma relação sobre V. Reciprocamente, se R é uma relação sobre um conjunto V, então $G(V, R)$ é um grafo orientado simples. Assim, o conceito de relações sobre um conjunto e o de grafos orientados simples é o mesmo. De fato, no Capítulo 2, já introduzimos o grafo orientado correspondente a uma relação sobre um conjunto.

Suponha que G é um grafo orientado simples com m vértices e que os vértices de G tenham sido ordenados, sendo chamados de $v_1, v_2, \ldots, v_m$. Então, a *matriz de adjacência* $A = [a_{ij}]$ de G é a matriz $m \times m$ definida como se segue.

$$a_{ij} = \begin{cases} 1 & \text{se há uma aresta } (v_i, v_j) \\ 0 & \text{caso contrário} \end{cases}$$

Tal matriz A, que contém entradas iguais apenas a 0 ou 1, é chamada de *matriz de bits* ou *matriz Booleana*. (Apesar de a matriz de adjacência de um grafo não orientado ser simétrica, isso não se aplica aqui para um grafo orientado.)

A matriz de adjacência A do grafo G depende da ordenação dos vértices de G. Contudo, as matrizes resultantes de duas ordenações distintas são intimamente relacionadas entre si no sentido de que se pode obter uma a partir da outra apenas trocando linhas e colunas. A menos que seja dito o contrário, assumimos que os vértices de nossa matriz têm uma ordem fixada.

Observação: A matriz de adjacência $A = [a_{ij}]$ pode ser estendida para grafos orientados com arestas paralelas, fazendo:

$$a_{ij} = \text{o número de arestas começando em } v_i \text{ e terminando em } v_j$$

Logo, as entradas de A são inteiros não negativos. Reciprocamente, toda matriz A $m \times m$ com entradas que sejam inteiros não negativos define univocamente um grafo orientado com m vértices.

Exemplo 9.6 Seja G o grafo orientado na Fig. 9-4(a) com vértices v_1, v_2, v_3, v_4. Então a matriz de adjacência A de G aparece na Fig. 9-4(b). Note que o número de 1's em A é igual ao número (oito) de arestas.

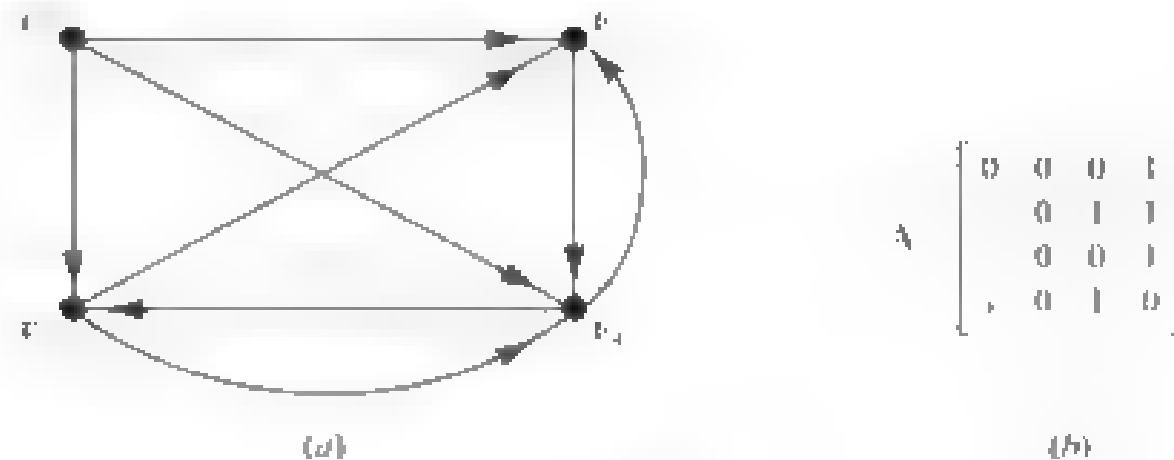



Figura 9-4

Considere as potências $A, A^2, A^3, \ldots$ da matriz de adjacência $A = [a_{ij}]$ de um grafo G. Faça

$$a_K(i, j) = \text{a entrada } ij \text{ da matriz } A^K$$

Observe que $a_1(i, j) = a_{ij}$ fornece o número de caminhos de comprimento 1 do vértice v_i ao vértice v_j. É possível mostrar que $a_2(i, j)$ fornece o número de caminhos de comprimento 2 de v_i a v_j. De fato, provamos no Problema 9.17 o seguinte resultado geral

Proposição 9.4: Seja A a matriz de adjacência de um grafo G. Então, $a_K(i, j)$, a entrada ij da matriz A^K, fornece o número de caminhos de comprimento K de v_i a v_j.

Exemplo 9.7 Considere novamente o grafo G e sua matriz de adjacência A que aparece na Fig. 9-4. As potências A^2, A^3 e A^4 de A são as que se seguem:

$$A^2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 2 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 2 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 1 & 0 & 0 & 2 \\ 3 & 0 & 2 & 3 \\ 2 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 2 & 0 & 2 & 1 \\ 5 & 0 & 3 & 5 \\ 3 & 0 & 2 & 3 \\ 3 & 0 & 1 & 4 \end{bmatrix}$$

Observe que $a_2(4, 1) = 1$ e, portanto, há um caminho de comprimento 2 de v_4 a v_1. Além disso, $a_3(2, 3) = 2$ e, portanto, há dois caminhos de comprimento 3 de v_2 a v_3; e $a_4(2, 4) = 5$, logo, existem cinco caminhos de comprimento 4 de v_2 a v_4.

Observação: Sejam A a matriz de adjacência de um grafo G e B_r a matriz definida por:

$$B_r = A + A^2 + A^3 + \cdots + A^r$$

Então a entrada ij da matriz B_r dá o número de caminhos de comprimento r, ou menos, do vértice v_i ao vértice v_j.

Matriz de caminhos

Seja $G = G(V, E)$ um grafo orientado simples com m vértices $v_1, v_2, \ldots, v_m$. A *matriz de caminhos* ou *matriz de alcançabilidade* de G é a matriz quadrada $P = [p_{ij}]$ de ordem m, definida como:

$$p_{ij} = \begin{cases} 1 & \text{se existe um caminho de } v_i \text{ a } v_j \\ 0 & \text{caso contrário} \end{cases}$$

(A matriz de caminhos P pode ser vista como o fecho transitivo da relação E sobre V.)

Suponha agora que existe um caminho do vértice v_i ao vértice v_j em um grafo com m vértices. Então deve haver um caminho simples de v_i a v_j quando $v_i \neq v_j$, ou um ciclo de v_i a v_j quando $v_i = v_j$. Como G tem m vértices, tal caminho simples deve ter comprimento $m - 1$ ou menor, ou tal ciclo deve ter comprimento menor ou igual a m. Isso significa que existe uma entrada ij não nula na matriz B_m (acima definida) onde A é a matriz de adjacência de G. Consequentemente, a matriz de caminhos P e B_m têm as mesmas entradas não nulas. Estabelecemos formalmente esse resultado.

Proposição 9.5: Seja A a matriz de adjacência de um grafo G com m vértices. Então P é fortemente conexo se, e somente se, B_m não tem entradas nulas, onde

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

Exemplo 9.8 Considere o grafo G e sua matriz de adjacência A que aparece na Fig. 9-4. Aqui G tem $m = 4$ vértices. Adicionando a matriz A às matrizes A^2, A^3 e A^4 no Exemplo 9.7, obtemos a seguinte matriz B_4, e também a matriz de caminhos (alcançabilidade) P, substituindo as entradas não nulas em B_4 por 1

$$B_4 = \begin{bmatrix} 4 & 0 & 3 & 4 \\ 11 & 0 & 7 & 11 \\ 7 & 0 & 4 & 7 \\ 7 & 0 & 4 & 7 \end{bmatrix} \quad \text{e} \quad P = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Examinando a matriz B_4 ou P, vemos entradas nulas; portanto, G não é fortemente conexo. Em especial, percebemos que o vértice v_2 não é alcançável a partir de qualquer um dos demais vértices.

Observação: A matriz de adjacência A e a matriz de caminhos P de um grafo G podem ser compreendidas como matrizes lógicas (Booleanas), onde 0 representa "falso" e 1 corresponde a "verdadeiro". Assim, as operações lógicas de $\wedge$ (AND) e $\vee$ (OR) podem ser aplicadas às entradas de A e P, de modo que essas operações, usadas na próxima seção, são definidas na Fig. 9-5.

$\wedge$	0	1
0	0	0
1	0	1

(a) AND.

$\vee$	0	1
0	0	1
1	1	1

(b) OR.

Figura 9-5

Fecho transitivo e a matriz de caminhos

Seja R uma relação sobre um conjunto finito V com m elementos. Como observado acima, a relação R pode ser identificada com o grafo orientado simples $G = G(V, R)$. Observamos que a relação de composição $R^2 = R \times R$ consiste em todos os pares (u, v) tais que existe um caminho de comprimento 2 de u a v. Analogamente:

$$R^K = \{(u, v) | \text{ existe um caminho de comprimento } K \text{ de } u \text{ a } v\}.$$

O fecho transitivo R^* da relação R sobre V pode agora ser visto como o conjunto de pares ordenados (u, v) tais que existe um caminho de u a v no grafo G. Além disso, de acordo com a discussão anterior, precisamos olhar apenas para os caminhos simples de comprimento $m - 1$ ou menor e os ciclos de comprimento m ou menor. Logo, temos o seguinte resultado que caracteriza o fecho transitivo R^* de R

Teorema 9.7: Seja R uma relação sobre um conjunto V com m elementos. Então:

(i) $R^* = R \cup R^2 \cup \ldots \cup R^m$ é o fecho transitivo de R.

(ii) A matriz de caminhos P de $G(V, R)$ é a matriz de adjacência de $G'(V, R^*)$.

9.6 ALGORITMO DE WARSHALL, CAMINHOS MAIS CURTOS

Seja G um grafo orientado com m vértices $v_1, v_2, \ldots, v_m$. Suponha que queremos encontrar a matriz de caminhos P do grafo G. Warshall deu um algoritmo que é muito mais eficiente do que calcular as potências da matriz de adjacência A. Esse algoritmo é definido nesta seção, e um algoritmo semelhante é empregado para encontrar os caminhos mais curtos em G, quando G é ponderado.

Algoritmo de Warshall

Primeiro definimos matrizes quadradas Booleanas de ordem m, $P_0, P_1, \ldots, P_m$, onde $P_k[i, j]$ denota a entrada ij da matriz P_k:

$$P_k[i,j] = \begin{cases} 1 & \text{se existe um caminho simples de } v_i \text{ a } v_j \text{ que não emprega quaisquer} \\ & \quad \text{outros vértices, exceto, possivelmente } v_1, v_2, \ldots, v_k. \\ 0 & \text{no caso contrário} \end{cases}$$

Por exemplo,

$$P_3[i,j] = 1 \text{ se há um caminho simples de } v_i \text{ a } v_j \text{ que não usa quaisquer outros vértices, exceto, possivelmente } v_1, v_2, v_3.$$

Note que a primeira matriz $P_0 = A$, a matriz de adjacência de G. Além disso, como G tem apenas m vértices, a última matriz $P_m = P$, a matriz de caminhos de G.

Warshall observou que $P_k[i, j] = 1$ pode ocorrer apenas se um dos dois casos a seguir acontecer:

(1) Existe um caminho simples de v_i a v_j que não usa quaisquer outros vértices, exceto, possivelmente $v_1, v_2, \ldots, v_{k-1}$, logo,

$$P_{k-1}[i,j] = 1$$

(2) Existe um caminho simples de v_i a v_k e um caminho simples de v_k a v_j, onde cada um deles não usa quaisquer outros vértices, exceto, possivelmente $v_1, v_2, \ldots, v_{k-1}$; logo,

$$P_{k-1}[i,k] = 1 \text{ e } P_{k-1}[k,j] = 1$$

Esses dois casos são descritos como se segue.

$$(1)\ v_i \to \cdots \to v_j; \qquad (2)\ v_i \to \cdots \to v_k \to \cdots v_j$$

onde $\to \cdots \to$ denota parte de um caminho simples que não emprega quaisquer outros vértices, exceto, possivelmente $v_1, v_2, \ldots, v_{k-1}$. Logo, os elementos de P_k podem ser obtidos por:

$$P_k[i,j] = P_{k-1}[i,j] \vee (P_{k-1}[i,k] \wedge P_{k-1}[k,j])$$

onde utilizamos as operações lógicas $\wedge$ (AND) e $\vee$ (OR). Em outras palavras, podemos obter cada entrada na matriz P_k, olhando apenas três entradas da matriz P_{k-1}. O algoritmo de Warshall aparece na Fig. 9-6.

Algoritmo 9.1 (Warshall): Um grafo orientado G com M vértices é mantido na memória por sua matriz de adjacência A. Esse algoritmo encontra a matriz de caminhos (Booleana) P do grafo G

Passo 1. Repetir para $I, J = 1, 2, \ldots, M$: [Inicializa P.]
Se $A[I, J] = 0$, então: Faça $P[I, J] := 0$;
Caso contrário: Faça $P[I, J] := 1$.
[Fim do ciclo.]

Passo 2. Repita os Passos 3 e 4 para $K = 1, 2, \ldots, M$: [Atualiza P.]

Passo 3. Repita o Passo 4 para $I = 1, 2, \ldots, M$:

Passo 4. Repita para $J = 1, 2, \ldots, M$
Faça $P[I, J] := P[I, J] \vee (P[I, K] \wedge (P[K, J])$.
[Fim do ciclo.]
[Fim do ciclo do Passo 3.]
[Fim do ciclo do Passo 2.]

Passo 5. Saída.

Figura 9-6

Algoritmo do caminho mais curto

Seja G um grafo orientado simples com m vértices $v_1, v_2, \ldots, v_m$. Suponha que G é ponderado, ou seja, que cada aresta e de G é assinalada com um número não negativo $w(e)$, chamado de *peso* ou *comprimento* de e. Então G pode ser mantido na memória por sua matriz de pesos $W = [w_{ij}]$, definida como se segue:

$$w_{ij} = \begin{cases} w(e) & \text{se existe uma aresta } e \text{ de } v_i \text{ a } v_j \\ 0 & \text{se não há aresta de } v_i \text{ a } v_j \end{cases}$$

A matriz de caminhos P nos diz se há caminhos entre os vértices. Agora queremos encontrar uma matriz Q que nos diz os comprimentos dos caminhos mais curtos entre os vértices ou, mais precisamente, uma matriz $Q = [q_{ij}]$ tal que

$$q_{ij} = \text{comprimento do caminho mais curto de } v_i \text{ a } v_j$$

A seguir descrevemos uma modificação do algoritmo de Warshall que eficientemente determina a matriz Q.

Definimos aqui uma sequência de matrizes $Q_0, Q_1, \ldots, Q_m$ (análogas às matrizes $P_0, P_1, \ldots, P_m$, dadas anteriormente) onde $Q_k[i, j]$, a entrada ij de Q_k, é definida como se segue:

$Q_k[i, j]$ = o menor dos valores entre o comprimento do caminho precedente de v_i a v_j e a soma dos comprimentos dos caminhos precedentes de v_i a v_k e de v_k a v_j.

Mais precisamente,

$$Q_k[i, j] = \text{MIN}(Q_{k-1}[i, j], Q_{k-1}[i, k] + Q_{k-1}[k, j])$$

A matriz inicial Q_0 é igual à matriz ponderada W, exceto pelo fato de que cada 0 em w é substituído por ∞ (ou um número muito, muito grande). A matriz final Q_m é a matriz desejada Q.

Exemplo 9.9 A Fig. 9-7 mostra um grafo ponderado G e sua matriz de pesos W, onde assumimos que $v_1 = R$, $v_2 = S$, $v_3 = T$, $v_4 = U$.

Suponha que aplicamos o algoritmo modificado de Warshall em nosso grafo ponderado G na Fig. 9-7. Obtemos as matrizes Q_0, Q_1, Q_3 e Q_4, na Fig. 9-8. (À direita de cada matriz Q_k, na Fig. 9-8, mostramos a matriz de caminhos que correspondem aos comprimentos da matriz Q_k.) As entradas na matriz Q_0 são as mesmas da matriz de

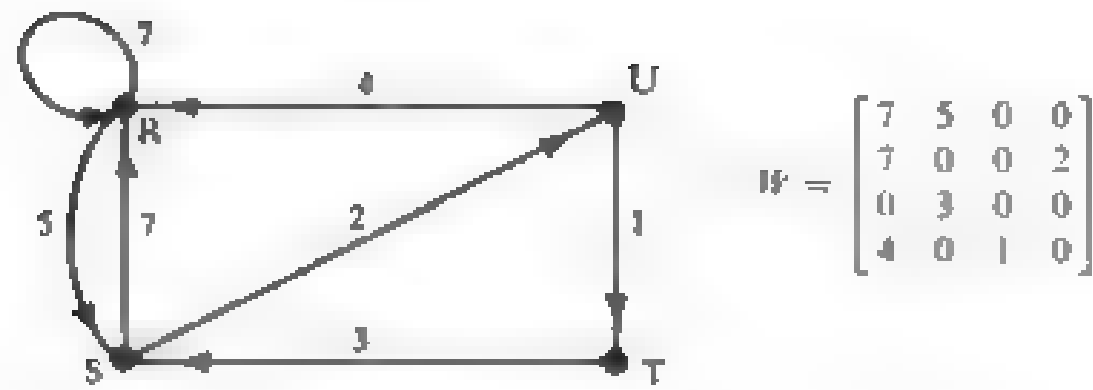



Figura 9-7

pesos W, exceto que cada 0 em W é substituído por ∞ (um número muito grande). Indicamos como as entradas circundadas são obtidas.

$$\begin{aligned}
Q_1[4,2] &= \text{MIN}\,(Q_0[4,2], & Q_0[4,1] + Q_0[1,2]) &= \text{MIN}(\infty, 4+5) = 9\\
Q_2[1,3] &= \text{MIN}\,(Q_1[1,3], & Q_1[1,2] + Q_1[2,3]) &= \text{MIN}(\infty, 5+\infty) = \infty\\
Q_3[4,2] &= \text{MIN}\,(Q_2[4,2], & Q_2[4,3] + Q_2[3,2]) &= \text{MIN}(9, 3+1) = 4\\
Q_4[3,1] &= \text{MIN}\,(Q_3[3,1], & Q_3[3,4] + Q_3[4,1]) &= \text{MIN}(10,5+4) = 9
\end{aligned}$$

A última matriz $Q_4 = Q$ é a procurada matriz de caminhos mais curtos.

$$Q_0 = \begin{bmatrix} 7 & 5 & \infty & \infty \\ 7 & \infty & \infty & 2 \\ \infty & 3 & \infty & \infty \\ 4 & \infty & 1 & \infty \end{bmatrix} \qquad \begin{bmatrix} RR & RS & — & — \\ SR & — & — & SU \\ — & TS & — & — \\ UR & — & UT & — \end{bmatrix}$$

$$Q_1 = \begin{bmatrix} 7 & 5 & \infty & \infty \\ 7 & 12 & \infty & 2 \\ \infty & 3 & \infty & \infty \\ 4 & \textcircled{9} & 1 & \infty \end{bmatrix} \qquad \begin{bmatrix} RR & RS & — & — \\ SR & SRS & — & SU \\ — & TS & — & — \\ UR & URS & UT & — \end{bmatrix}$$

$$Q_2 = \begin{bmatrix} 7 & 5 & \textcircled{∞} & 7 \\ 7 & 12 & \infty & 2 \\ 10 & 3 & \infty & 5 \\ 4 & 9 & 1 & 11 \end{bmatrix} \qquad \begin{bmatrix} RR & RS & — & RSU \\ SR & SRS & — & SU \\ TSR & TS & — & TSU \\ UR & URS & UT & URS \end{bmatrix}$$

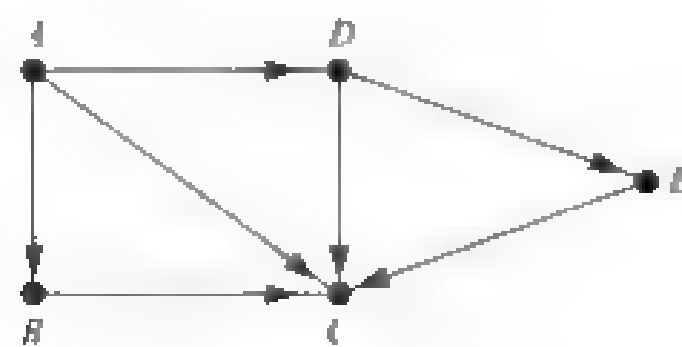
$$Q_3 = \begin{bmatrix} 7 & 5 & \infty & 7 \\ 7 & 12 & \infty & 2 \\ 10 & 3 & \infty & 5 \\ 4 & \textcircled{4} & 1 & 6 \end{bmatrix} \qquad \begin{bmatrix} RR & RS & — & RSU \\ SR & SRS & — & SU \\ TSR & TS & — & TSU \\ UR & UTS & UT & UTSU \end{bmatrix}$$

$$Q_4 = \begin{bmatrix} 7 & 5 & 8 & 7 \\ 7 & 11 & 3 & 2 \\ \textcircled{9} & 3 & 6 & 5 \\ 4 & 4 & 1 & 6 \end{bmatrix} \qquad \begin{bmatrix} RR & RS & RSUT & RSU \\ SR & SURS & SUT & SU \\ TSUR & TS & TSUT & TSU \\ UR & UTS & UT & UTSU \end{bmatrix}$$

Figura 9-8

9.7 REPRESENTAÇÃO LIGADA DE GRAFOS ORIENTADOS

Seja G um grafo orientado com m vértices. Suponha que o número de arestas de G é de ordem $O(m)$ ou mesmo $O(m \log m)$, ou seja, suponha que G é esparso. Então a matriz de adjacência A de G contém muitos zeros, logo, muita

memória é desperdiçada. Consequentemente, quando G é esparso, G em geral é representado na memória por algum tipo de *representação ligada*, também conhecida como estrutura de adjacência, a qual é descrita abaixo por meio de um exemplo.

(*a*) Grafo G

Vértice	Lista de adjacência
A	B, C, D
B	C
C	$\varnothing$
D	C, E
E	C

(*b*) Listas de adjacência de G

Figura 9-9

Considere o grafo orientado G na Fig. 9-9(*a*). Observe que G pode ser equivalentemente definido pela tabela da Fig. 9-9(*b*), que mostra cada vértice de G seguido por sua *lista de adjacência*, também conhecida como lista de *sucessores* ou *vizinhos*. Aqui o símbolo $\varnothing$ denota uma lista vazia. Note que cada aresta de G corresponde a um único vértice em uma lista de adjacência e vice-versa. Aqui G tem sete arestas e existem sete vértices nas listas de adjacência. Essa tabela pode ser apresentada também da seguinte maneira compacta, onde dois pontos ":" separam um vértice de sua lista de vizinhos, e ponto e vírgula ";" separa as diferentes listas.

$$G = [A : B, C, D; \quad B : C; \quad C : \varnothing; \quad D : C, E; \quad E : C]$$

A *representação ligada* de um grafo orientado G mantém G na memória, usando listas ligadas para suas listas de adjacência. Especificamente, a representação ligada de modo geral contém dois arquivos (conjuntos de registros), sendo um conhecido como Arquivo de Vértices e o outro, como Arquivo de Arestas, da seguinte maneira.

(a) ***Arquivo de Vértices***: O Arquivo de Vértices contém a lista de vértices do grafo G, geralmente mantido por um array ou uma lista ligada. Cada registro do Arquivo de Vértices tem a forma

VERTEX	NEXT-V	PTR	

Aqui VERTEX é o nome do vértice, NEXT-V aponta para o próximo vértice na lista de vértices do arquivo, e PTR aponta para o primeiro elemento na lista de adjacência do vértice que aparece no Arquivo de Arestas. A área sombreada indica que pode haver outra informação no registro correspondente ao vértice

(b) ***Arquivo de Arestas***: O Arquivo de Arestas contém as arestas de G e também todas as listas de adjacência de G, onde cada lista é mantida na memória por uma lista ligada. Cada registro do arquivo representa uma única aresta de G e, portanto, corresponde a um único vértice em uma lista de adjacência. O registro geralmente tem a forma

Aqui:

(1) EDGE é o nome da aresta (se tiver um).

(2) BEG-V aponta para a localização no Arquivo de Vértices do vértice inicial da aresta.

(3) END-V aponta para a localização no Arquivo de Vértices do vértice terminal da aresta. As listas de adjacência aparecem nesse campo.

(4) NEXT-E aponta para a localização no Arquivo de Arestas do próximo vértice na lista de adjacência.

Enfatizamos que as listas de adjacência consistem em vértices terminais e, portanto, são mantidas pelo campo END-V. A área sombreada indica que pode haver outra informação correspondente à aresta. Notamos que a ordem dos vértices em qualquer lista de adjacência depende da ordem na qual as arestas (pares de vértices) aparecem na entrada (*input*).

A Fig. 9-10 mostra como o grafo G na Fig. 9-9(a) pode aparecer na memória. Aqui os vértices de G são mantidos na memória por uma lista ligada, usando a variável START para apontar para o primeiro vértice. (Alternativamente, pode-se usar um array linear para a lista de vértices e, em então, NEXT-V não é necessário.) A escolha de oito localizações para o Arquivo de Vértices e 10 localizações para o Arquivo de Arestas é arbitrária. O espaço adicional nos arquivos é usado se vértices ou arestas extras são inseridos no grafo. A Fig. 9-10 também mostra, com flechas, a lista de adjacência $[B, C, D]$ do vértice A.

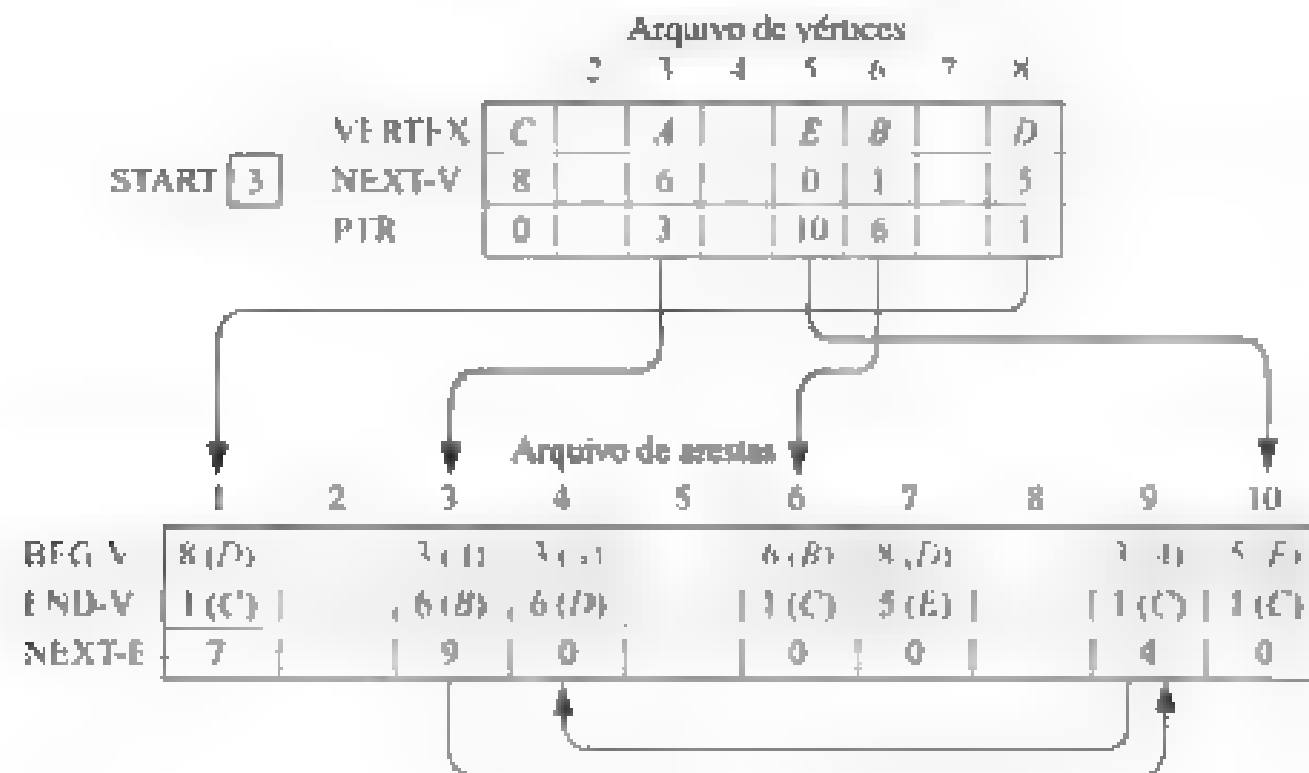



Figura 9-10

9.8 ALGORITMOS DE GRAFOS: BUSCA EM PROFUNDIDADE E BUSCA EM LARGURA

Esta seção discute dois algoritmos importantes para um dado grafo G. Qualquer algoritmo de um grafo em particular pode depender da maneira como G é mantido na memória. Assumimos aqui que G é mantido na memória por sua estrutura de adjacência. Nosso grafo de teste G com sua lista estrutura de adjacência aparece na Fig. 9-11.

Muitas aplicações de grafos exigem um exame sistemático dos vértices e arestas de um grafo G. Há duas maneiras usuais para isso ser feito. Uma é chamada de *busca em profundidade* (DFS) e a outra, de *busca em largura* (BFS). (Esses algoritmos são essencialmente idênticos aos algoritmos análogos para grafos não orientados do Capítulo 8.)

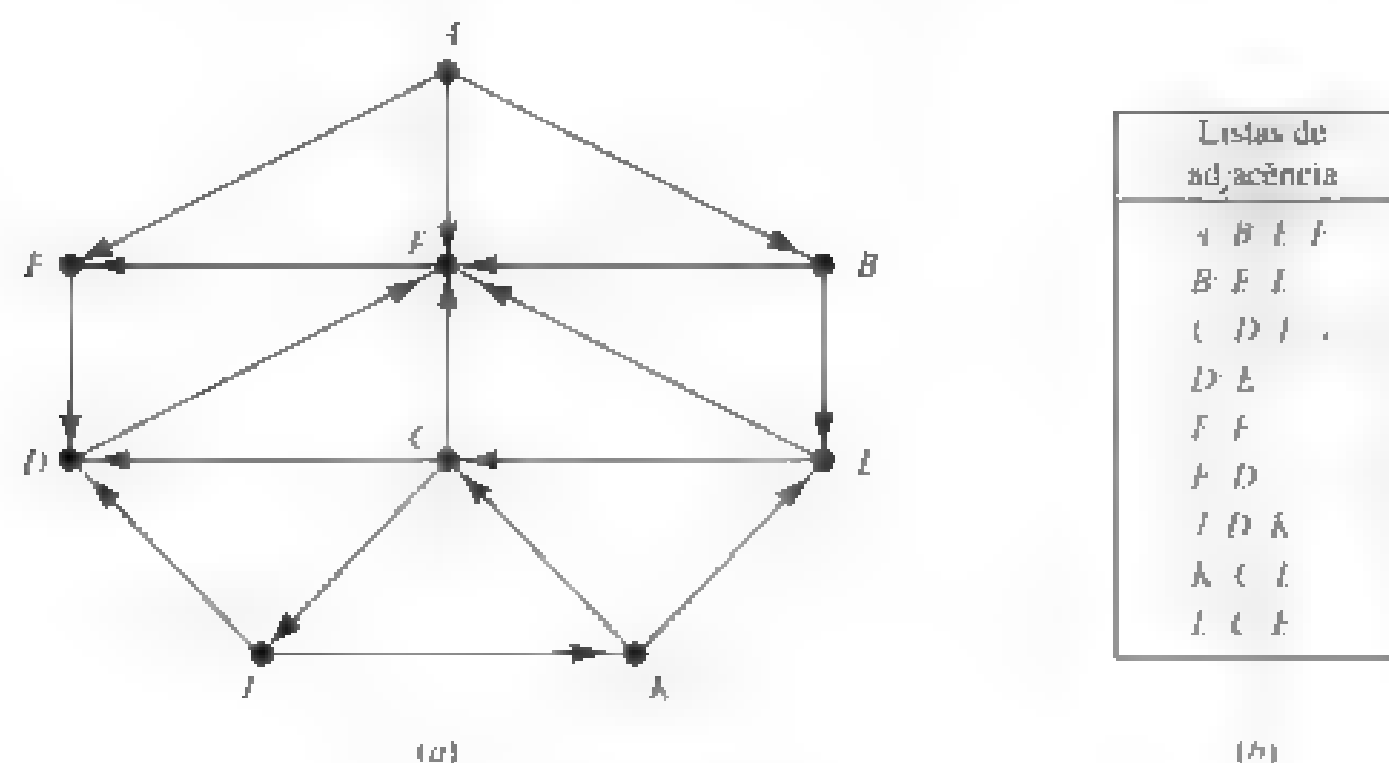



Figura 9-11

Durante a execução de nossos algoritmos, cada vértice (nó) *N* de *G* estará em um de três estados, chamados de *status* de *N*, como se segue:

STATUS = 1: (Estado Pronto) O estado inicial do vértice *N*.

STATUS = 2: (Estado de Espera) O vértice *N* está em uma lista (de espera), aguardando para ser processado.

STATUS = 3: (Estado Processado) O vértice *N* foi processado.

A lista de espera para a busca em profundidade é uma PILHA (modificada, a qual escrevemos horizontalmente com o TOPO da PILHA à esquerda), enquanto a lista de espera para a busca em largura é uma FILA.

(a) **Busca em profundidade:** A ideia geral por trás de uma busca em profundidade começando em um vértice inicial *A* é como se segue. Primeiro, processamos o vértice inicial *A*. Em seguida, processamos cada vértice *N* ao longo de um caminho *P* que começa em *A*, ou seja, processamos um vizinho de *A*, depois um vizinho de um vizinho de *A*, e assim por diante. Depois de chegarmos a um "beco sem saída", isto é, a um vértice sem vizinho não processado, voltamos pelo caminho *P* até ser possível continuar por outro caminho P', e assim por diante. O retorno é realizado, usando uma PILHA para manter os vértices iniciais de futuros caminhos possíveis. Também precisamos de um campo STATUS que nos diga o estado atual de qualquer vértice, de modo que nenhum vértice é processado mais de uma vez. O algoritmo aparece na Fig. 9-12.

Algoritmo 9.2 (busca em profundidade): Esse algoritmo executa uma busca em profundidade sobre um grafo orientado *G* começando com um vértice inicial *A*.

Passo 1. Inicialize todos os vértices com o estado pronto (STATUS = 1)

Passo 2. Jogue o vértice inicial *A* em PILHA e mude o estado de *A* para o modo de espera (STATUS = 2).

Passo 3. Repita os Passos 4 e 5 até PILHA estar vazia.

Passo 4. Mova o vértice *N* do topo de PILHA. Processe *N* e faça STATUS(*N*) = 3, o estado processado.

Passo 5. Examine cada vizinho *J* de *N*.

(*a*) Se STATUS (*J*) = 1 (estado pronto), jogue *J* em PILHA e mude STATUS (*J*) = 2 (estado de espera)

(*b*) Se STATUS (*J*) = 2 (estado de espera), delete o *J* anterior de PILHA e jogue o atual *J* em PILHA.

(*c*) Se STATUS (*J*) = 3 (estado processado), ignore o vértice *J*.

[Fim do ciclo do Passo 3.]

Passo 6. Saída.

Figura 9-12

O algoritmo 9.2 processa apenas aqueles vértices que são alcançáveis a partir de um vértice inicial *A*. Suponha que queremos processar todos os vértices no grafo *G*. Então o algoritmo deve ser modificado, de modo que comece novamente com outro vértice que ainda esteja no estado pronto (STATUS = 1). Esse novo vértice, digamos *B*, pode ser obtido, investigando ao longo da lista de vértices.

Observação: A estrutura PILHA no Algoritmo 9.2 não é tecnicamente uma pilha, pois, no Passo 5(*b*), permitimos que um vértice *J* seja deletado e então inserido na frente de pilha. (Apesar de ser o mesmo vértice, ele representa uma aresta diferente.) Se não deletarmos o *J* anterior no Passo 5(*b*), então obtemos um algoritmo de passagem alternativo.

Exemplo 9.10 Considere nosso grafo de teste *G* na Fig. 9-11. Suponha que queremos encontrar e imprimir todos os vértices alcançáveis a partir de *J* (incluindo o próprio *J*). Uma maneira de fazer isso é usando uma busca em profundidade de *G* começando no vértice *J*.

Aplicando o Algoritmo 9.2, os vértices serão processados e impressos na seguinte ordem:

$$J, K, L, E, F, D, C$$

Especificamente, a Fig. 9-13(*a*) mostra a sequência de listas de espera em PILHA e os vértices sendo processados (A barra / indica que o vértice é deletado da lista de espera.) Enfatizamos que cada vértice, excluindo J, vem de uma lista de adjacência e, portanto, cada um é vértice terminal de uma única aresta do grafo. Indicamos a aresta, rotulando o vértice terminal com o vértice inicial da aresta, na forma de um subscrito. Por exemplo,

$$D_J$$

significa que D está na lista de adjacência de J e, portanto, D é o vértice terminal de uma aresta que começa em J. Essas arestas formam uma árvore T com raiz J, a qual é retratada na Fig. 9-13(*b*). (Os números indicam a ordem em que as arestas são adicionadas à árvore.) Essa árvore T gera o subgrafo G' de G que consiste em vértices alcançáveis a partir de J.

PILHA	Vértice
J	J
K_J, D_J	K_J
L_K, C_K, D_J	L_K
E_L, C_L, C_K, D_J	E_L
F_E, C_L, D_J	F_E
D_F, C_L, B_J |	D_F
C_L |	C_L
$\varnothing$	

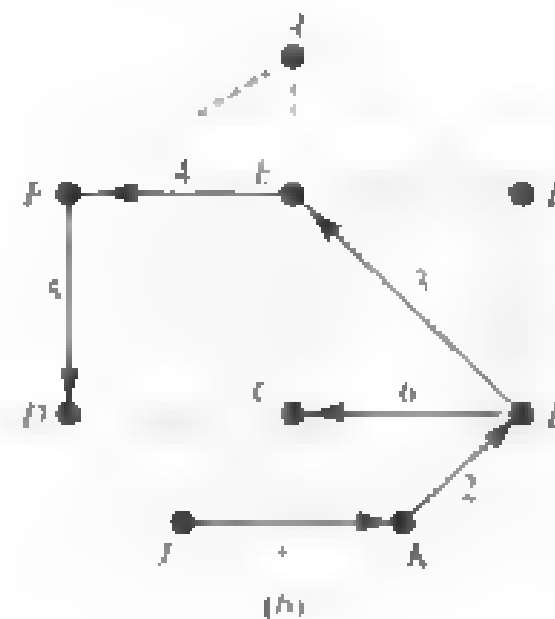
(*a*)

(*b*)

Figura 9-13

(b) **Busca em largura:** A ideia geral por trás de uma busca em largura que começa em um vértice inicial A é como se segue. Primeiro, processamos o vértice inicial A. Em seguida, processamos todos os vizinhos de A. Então processamos todos os vizinhos dos vizinhos de A, e assim por diante. Naturalmente, precisamos acompanhar os vizinhos de um vértice e garantir que nenhum vértice seja processado duas vezes. Isso se consegue usando uma FILA para manter os vértices que estão esperando para serem processados; e por meio de um campo STATUS que nos diz o estado atual de um vértice. O algoritmo aparece na Fig. 9-14.

O Algoritmo 9.3 processa apenas aqueles vértices que são alcançáveis a partir de um A inicial. Suponha que se queira processar todos os vértices no grafo G. Então o algoritmo deve ser modificado, de modo que comece novamente com outro vértice que ainda esteja no estado pronto (STATUS = 1). Esse novo vértice, digamos B, pode ser obtido, examinando a lista de vértices.

Exemplo 9.11 Considere nosso grafo de teste G na Fig. 9-11. Suponha que G representa os voos diários entre cidades e que desejamos voar da cidade A para a cidade J com o menor número de paradas. Ou seja, queremos encontrar um caminho mais curto P de A a J (onde cada aresta tem peso 1). Uma maneira de fazer isso é usar a busca em largura de G começando no vértice A e parar assim que J seja encontrado.

A Fig. 9-15(*a*) mostra a sequência de listas de espera na FILA e os vértices sendo processados até o momento em que J é encontrado. Então trabalhamos de trás para frente, a partir de J, para obter o próximo caminho desejado, que é retratado na Fig. 9-15(*b*):

$$J_C \leftarrow C_L \leftarrow L_B \leftarrow B_A \leftarrow A \text{ ou } A \rightarrow B \rightarrow L \rightarrow C \rightarrow J$$

Logo, um voo da cidade A para a cidade J fará três paradas intermediárias em B, L e C. Observe que o caminho não inclui todos os vértices processados pelo algoritmo.

Algoritmo 9.3 (busca em largura): Esse algoritmo executa uma busca em largura sobre um grafo orientado G começando com um vértice inicial A.

Passo 1. Inicialize todos os vértices com o estado pronto (STATUS = 1).

Passo 2. Coloque o vértice inicial A em FILA e mude o estado de A para o modo de espera (STATUS = 2).

Passo 3. Repita os Passos 4 e 5 até FILA estar vazia.

Passo 4. Remova o primeiro vértice N de FILA. Processe N e faça STATUS (N) = 3, o estado processado.

Passo 5. Examine cada vizinho J de N.

(*a*) Se STATUS (J) = 1 (estado pronto), adicione J para o fim de FILA e faça STATUS (J) = 2 (estado de espera).

(b) Se STATUS (J) 2 (estado de espera) ou STATUS (J) 3 (estado processado), ignore o vértice J.

[Fim do ciclo do Passo 3.]

Passo 6. Saída.

Figura 9-14

FILA	Vértice
A	A
F_A, E_A, B_A	B_A
L_B, F_A, E_A	E_A
L_B, F_A	F_A
D_F, L_B	L_B
C_L, D_F	D_F
C_L	C_L
J_C	J_C

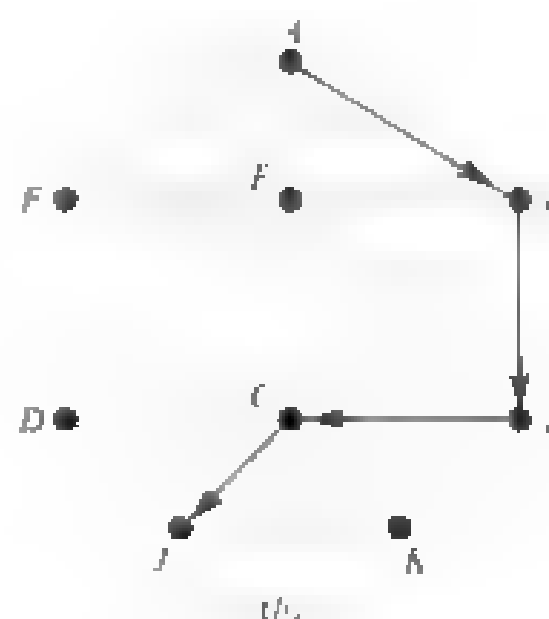



Figura 9-15

9.9 GRAFOS ORIENTADOS LIVRES DE CICLOS, ORDENAÇÃO TOPOLÓGICA

Seja S um grafo orientado com as duas propriedades a seguir:

(1) Cada vértice v_i de S representa uma tarefa.

(2) Cada aresta (orientado) (u, v) de S significa que a tarefa u deve ser completada antes de iniciar a tarefa v.

Observamos que tal grafo S não pode conter um ciclo, como $P = (u, v, w, u)$, pois, caso contrário, teríamos que completar u antes de começar v, completar v antes de começar v e completar w antes de começar u. Ou seja, não podemos começar qualquer uma das três tarefas no ciclo.

Tal grafo S, que representa tarefas e uma relação de pré-requisitos, e que não pode ter qualquer ciclo, é dito *livre de ciclos* ou *acíclico*. Um grafo orientado acíclico (livre de ciclos) é chamado abreviadamente de *dag* (sigla em inglês). A Fig. 9-16 é um exemplo de tal grafo.

Listas de adjacência	
A	C
B	D, F
C	
D	C
E	C
F	
G	A, F

(*a*) (*b*)

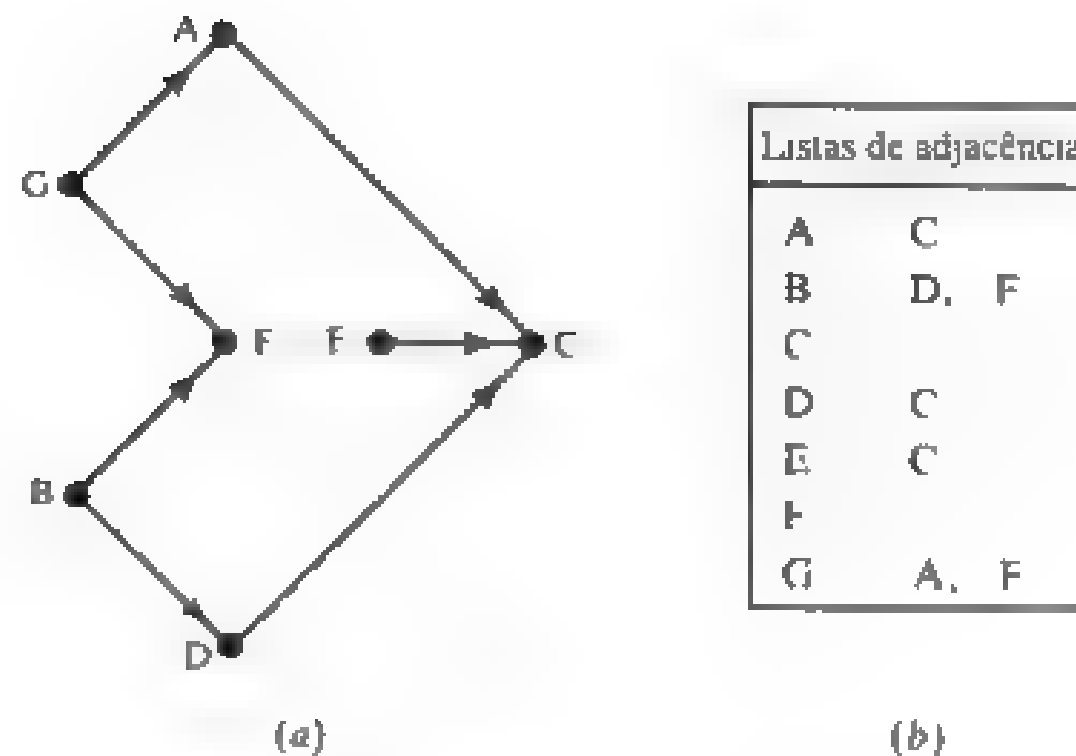



Figura 9-16

Uma operação fundamental sobre um dag *S* é processar os vértices um após o outro, de modo que o vértice *u* é sempre processado antes de *v*, se (u, v) é uma aresta. Tal ordem linear *T* dos vértices de *S*, que pode ser única, é chamada de ***ordenação topológica***.

A Fig. 9-17 mostra duas ordenações topológicas do grafo *S* da Fig. 9-16. Incluímos as arestas de *S* na Fig. 9-17 para mostrar que elas concordam com a orientação da ordem linear.

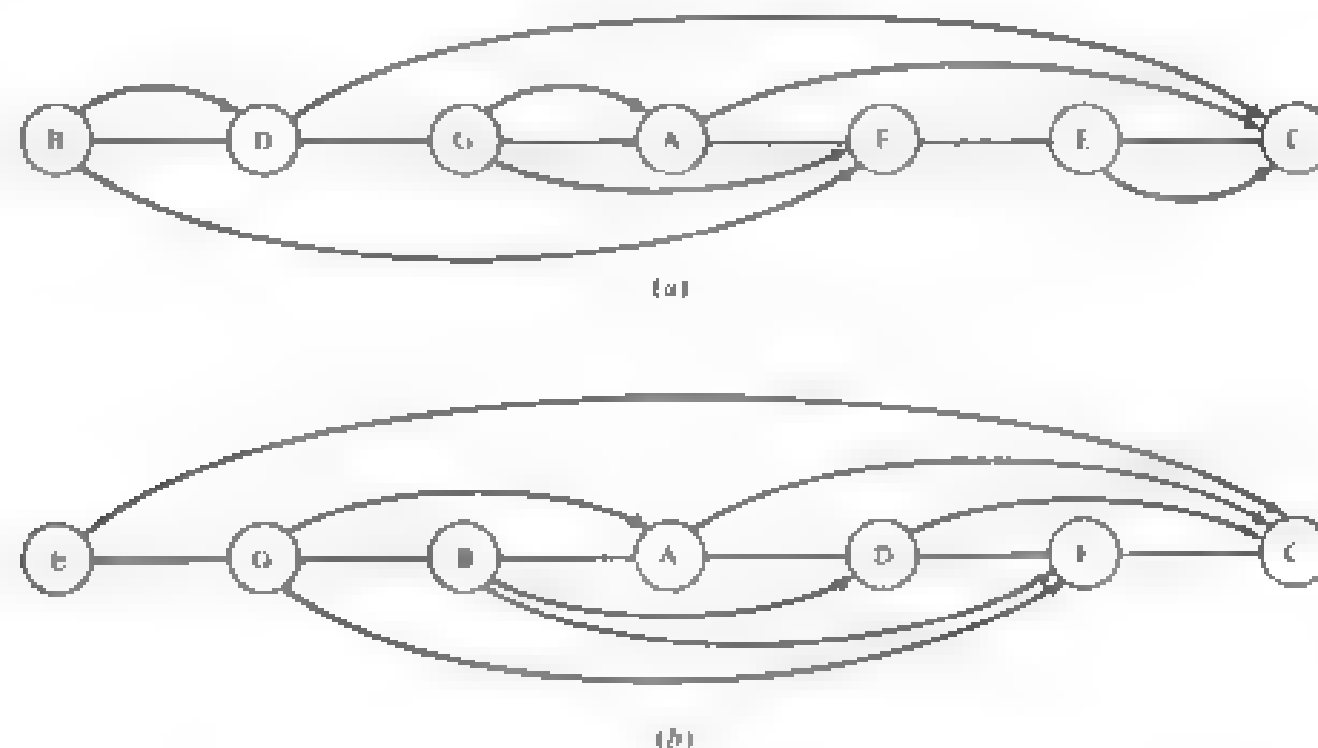



Figura 9-17 Duas ordenações topológicas.

O que se segue é o principal resultado teórico desta seção.

Teorema 9.8: Seja *S* um grafo orientado livre de ciclos. Então existe uma ordenação topológica *T* do grafo *S*.

Note que o teorema simplesmente estabelece que existe uma ordenação topológica. Agora fornecemos um algoritmo que encontra uma ordenação topológica. A ideia principal do algoritmo é que qualquer vértice (nó) *N* com grau de entrada nulo pode ser escolhido como o primeiro elemento na ordenação *T*. O algoritmo essencialmente repete os dois passos a seguir até *S* estar vazio:

(1) Encontre um vértice *N* com grau de entrada zero.

(2) Delete *N* e suas arestas do grafo *S*.

Usamos uma FILA auxiliar para manter temporariamente todos os vértices com grau nulo. O algoritmo aparece na Fig. 9-18.

Algoritmo 9.4: O algoritmo encontra uma ordenação topológica T de um grafo orientado livre de ciclos S.

Passo 1. Encontre o grau de entrada INDEG (N) de cada vértice N de S.

Passo 2. Insira em FILA todos os vértices com grau zero.

Passo 3. Repita os Passos 4 e 5 até FILA estar vazia.

Passo 4. Remova e processe o vértice frontal N de FILA.

Passo 5. Repita para cada vizinho M do vértice N.

(*a*) Faça INDEG(M) : = INDEG(M) − 1.
[Isso deleta a aresta de N à M.]

(*b*) Se INDEG(M) = 0, adicione M à FILA.

[Fim do ciclo.]

[Fim do ciclo do Passo 3.]

Passo 6. Saída.

Figura 9-18

Exemplo 9.12 Suponha que o Algoritmo 9.4 seja aplicado no grafo S da Fig. 9-16. Obtemos as seguintes sequências de elementos de FILA e de vértices sendo processados.

FILA	*GEB*	*DGE*	*DG*	*FAD*	*FA*	*CF*	*C*	∅
Vértice	*B*	*E*	*G*	*D*	*A*	*F*	*C*	

Assim, os vértices são processados na ordem: B, E, G, D, A, F.

9.10 ALGORITMOS DE PODA PARA CAMINHO MAIS CURTO

Seja G um grafo orientado livre de ciclos e ponderado. Buscamos pelo caminho mais curto entre dois vértices, digamos u e w. Assumimos que G é finito, de modo que em cada passo existe um número finito de movimentos. Como G é livre de ciclos, todos os caminhos entre u e w podem ser dados por uma árvore na qual u é a raiz. A Fig. 9-19(*b*) enumera todos os caminhos entre u e w no grafo da Fig. 9-19(*a*).

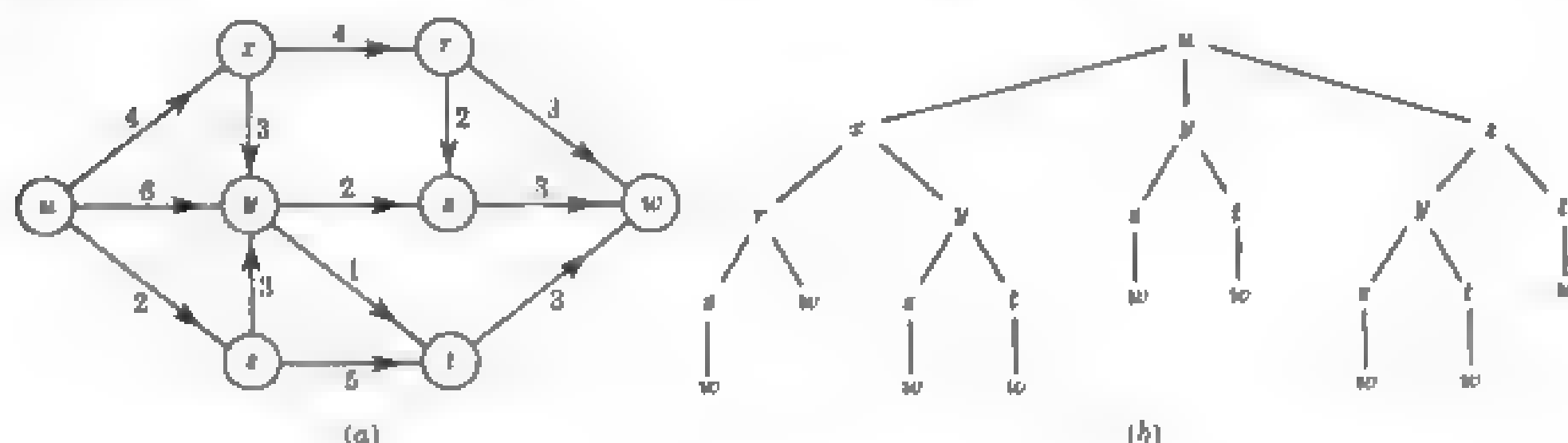



Figura 9-19

Uma maneira para encontrar o caminho mais curto entre u e w é simplesmente calculando os comprimentos de todos os caminhos da árvore enraizada correspondente. Por outro lado, suponha que dois caminhos parciais conduzam a um vértice intermediário v. A partir de então, precisamos apenas considerar o caminho parcial mais curto, ou seja, podamos a árvore no vértice correspondente ao caminho parcial mais longo. Esse algoritmo de poda é descrito a seguir.

Algoritmo de poda

Esse algoritmo encontra o caminho mais curto entre um vértice u e um vértice w em um grafo G orientado livre de ciclos e ponderado. O algoritmo tem as seguintes propriedades:

(a) Durante a execução, cada vértice v' de G é assinalado a duas coisas

  (1) Um número $\ell(v')$ denotando o atual comprimento mínimo de um caminho de u a v'

  (2) Um caminho $p(v')$ de u a v' com comprimento $\ell(v')$.

(b) Inicialmente, fazemos $\ell(u) = 0$ e $p(u) = u$. Todos os outros vértices v são inicialmente assinalados com $\ell(v) = \infty$ e $p(v) = \varnothing$

(c) Cada passo do algoritmo examina uma aresta $e = (v', v)$ de v' a v com, digamos, comprimento k. Calculamos $\ell(v') + k$.

  (1) Suponha que $\ell(v') + k < \ell(v)$. Então encontramos um caminho mais curto de u a v. Assim, atualizamos:

$$\ell(v) = \ell(v') + k \text{ e } p(v) = p(v')v$$

  (Isso é sempre verdade quando $\ell(v) = \infty$, ou seja, quando entramos primeiro com o vértice v.)

  (2) Caso contrário, não alteramos $\ell(v)$ e $p(v)$.

  Se nenhuma outra aresta não examinada entra com v, dizemos que $p(v)$ foi determinada.

(d) O algoritmo termina quando $p(w)$ é determinado.

Observação: A aresta $e = (v', v)$ em (c) somente pode ser escolhida se v' foi previamente visitada, ou seja, se $p(v')$ não está vazia. Além disso, geralmente é melhor examinar uma aresta que começa em um vértice v' cujo caminho $p(v')$ foi determinado.

Exemplo 9.13 Aplicamos o algoritmo de poda ao grafo G da Fig. 9-19(a).

A partir de u: Os vértices sucessivos são x, y e z, os quais são todos inseridos pela primeira vez. Logo:

  (1) faça $\ell(x) = 4$, $p(x) = ux$.

  (2) faça $\ell(y) = 6$, $p(y) = uy$

  (3) faça $\ell(z) = 2$, $p(z) = uz$.

  Note que $p(x)$ e $p(z)$ foram determinados.

A partir de x: Os vértices sucessivos são r, inserido pela primeira vez, e y. Logo:

  (1) faça $\ell(r) = 4 + 4 = 8$ e $p(r) = p(x)r = uxr$

  (2) Calculamos:

$$\ell(x) + k = 4 + 3 = 7 \text{ que não é menor do que } \ell(y) = 6.$$

  Assim, deixamos $\ell(y)$ e $p(y)$ como estão.

  Note que $p(r)$ foi determinado.

A partir de z: Os vértice sucessivos são t, inserido pela primeira vez, e y. Logo:

  (1) Faça $\ell(t) = \ell(z) + k = 2 + 5 = 7$ e $p(t) = p(z)t = uzt$

  (2) Calculamos:

$$\ell(z) + k = 2 + 3 = 5 \text{ que é menor do que } \ell(y) = 6.$$

  Encontramos um caminho mais curto para y e, assim, atualizamos $\ell(y)$ e $p(y)$, faça:

$$\ell(y) = \ell(z) + k = 5 \text{ e } p(y) = p(z)y = uzy.$$

  Agora $p(y)$ foi determinado.

A partir de *y*: Os vértices sucessivos são s, inserido pela primeira vez, e t. Logo:

(1) Fazemos $\ell(s) = \ell(y) + k = 5 + 2 = 7$ e $p(s) = p(y)s = uzys$.

(2) Calculamos:

$$\ell(y) + k = 5 + 1 = 6, \text{ que é menor do que } \ell(t) = 7.$$

Logo, mudamos $\ell(t)$ e $p(t)$ para:

$$\ell(t) = \ell(y) + 1 = 6 \text{ e } p(t) = p(y)t = uzyt.$$

Agora $p(t)$ foi determinado.

A partir de *r*: Os vértices sucessivos são w, inserido pela primeira vez, e s. Assim:

(1) Fazemos $\ell(w) = \ell(r) + 3 = 11$ e $p(w) = p(r)w = uxrw$

(2) Calculamos:

$$\ell(r) + k = 8 + 2 = 10 \text{ que não é menor do que } \ell(s) = 7.$$

Logo, deixamos $\ell(s)$ e $p(s)$ como estão.

Note que $p(s)$ foi determinado.

A partir de *s*: O vértice sucessivo é w. Calculamos:

$$\ell(s) + k = 7 + 3 = 10 \text{ que é menor do que } \ell(w) = 11.$$

Logo, mudamos $\ell(w)$ e $p(w)$ para:

$$\ell(w) = \ell(s) + 3 = 10 \text{ e } p(w) = p(s)w = uzysw.$$

A partir de *t*: O vértice sucessivo é w. Calculamos:

$$\ell(t) + k = 6 + 3 = 9 \text{ que é menor do que } \ell(w) = 10.$$

Logo, atualizamos $\ell(w)$ e $p(w)$ como se segue:

$$\ell(w) = \ell(t) + 3 = 9 \text{ e } p(w) = p(t) = uzytw.$$

Agora $p(w)$ foi determinado.

O algoritmo é encerrado, pois $p(w)$ foi determinado. Portanto, $p(w) = uzytw$ é o caminho mais curto de u a w e $\ell(w) = 9$.

As arestas que foram examinadas no exemplo acima formam a árvore enraizada da Fig. 9-20. Essa é a árvore na Fig. 9-19(b) que foi podada nos vértices pertencentes a caminhos parciais mais longos. Observe que apenas 13 das 23 arestas originais da árvore tiveram que ser examinadas.

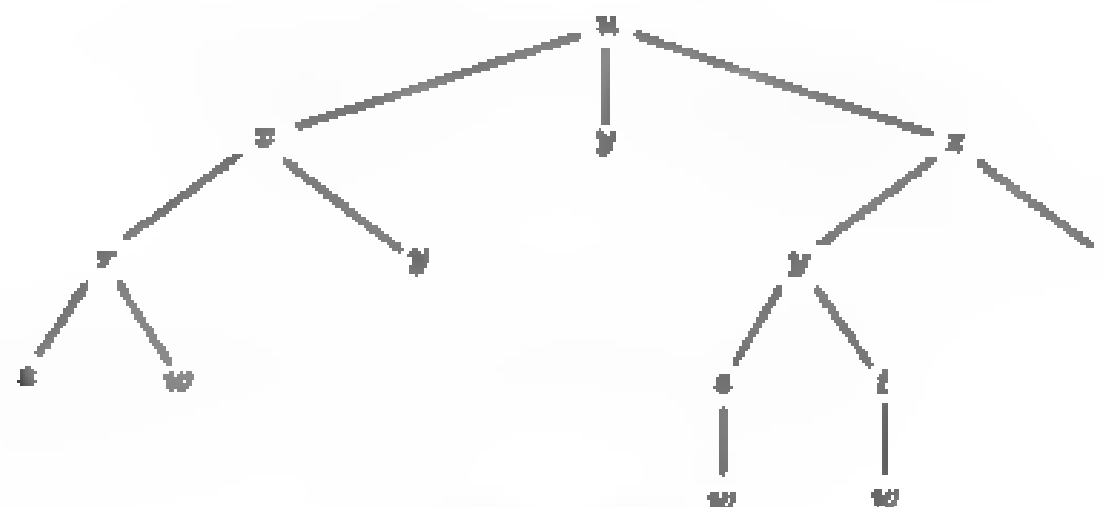



Figura 9-20

Problemas Resolvidos

Terminologia para grafos

9.1 Seja G o grafo orientado na Fig. 9-21(a).

(a) Descreva formalmente G.

(b) Encontre todos os caminhos simples de X a Z.

(c) Encontre todos os caminhos simples de Y a Z.

(d) Encontre todos os ciclos de G

(e) G é unilateralmente conexo?

(f) G é fortemente conexo?

(a) O conjunto V de vértices tem quatro vértices e o conjunto E de arestas (orientadas) tem sete arestas, como se segue

$$V = \{X, Y, Z, W\} \text{ e } E = \{(X, Y), (X, Z), (X, W), (Y, W), (Z, Y), (Z, W), (W, Z)\}$$

(b) Há três caminhos simples de X a Z, que são (X, Z), (X, W, Z) e (X, Y, W, Z).

(c) Existe apenas um caminho simples de Y a Z, que é (Y, W, Z).

(d) Há somente um ciclo em G, que é (Y, W, Z, Y).

(e) G é unilateralmente conexo, uma vez que (X, Y, W, Z) é um caminho gerador

(f) G não é fortemente conexo, pois não há caminho gerador fechado.

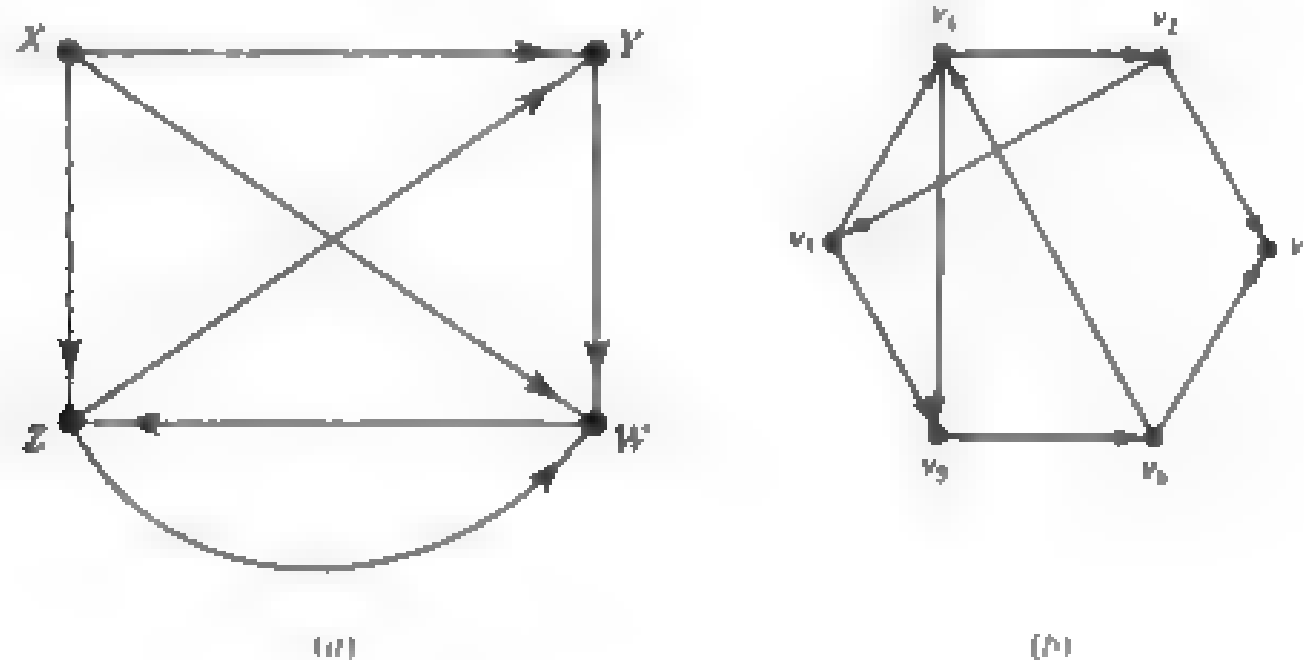



Figura 9-21

9.2 Seja G o grafo orientado na Fig. 9-21(a).

(a) Encontre o grau de entrada e o grau de saída de cada vértice de G.

(b) Encontre a lista de sucessores de cada vértice de G.

(c) Há quaisquer fontes ou poços?

(d) Encontre o subgrafo H de G determinado pelo conjunto de vértices $V' = X, Y, Z$.

(a) Conte o número de arestas terminando e começando em um vértice v, para obter, respectivamente, indeg(v) e outdeg(v). Isso nos leva aos dados:

$$\text{indeg}(X) = 0, \quad \text{indeg}(Y) = 2, \quad \text{indeg}(Z) = 2, \quad \text{indeg}(W) = 3$$
$$\text{outdeg}(X) = 3, \quad \text{outdeg}(Y) = 1, \quad \text{outdeg}(Z) = 2, \quad \text{outdeg}(W) = 1$$

(Como esperado, a soma dos graus de entrada e a soma dos graus de saída é, cada uma, 7, o número de arestas.)

(b) Adicione o vértice v à lista de sucessores succ(u) de u para cada aresta (u, v) em G. Isso nos leva a:

$$\text{succ}(X) = [Y, Z, W], \text{succ}(Y) = [W], \text{succ}(Z) = [Y, W], \text{succ}(W) = [Z]$$

(*c*) X é uma fonte, nenhuma aresta se dirige a ele, ou seja, $\text{indeg}(X) = 0$. Não há poços, pois todo vértice é o ponto inicial de uma aresta, isto é, tem outdegree não nulo.

(*d*) Seja E' o conjunto de todas as arestas de G cujos pontos terminais estão em V'. Isso nos leva a $E' = \{(X, Y), (X, Z), (Z, Y)\}$. Logo, $H = H(V', E')$.

9.3 Seja G o grafo orientado na Fig. 9-21(*b*).

(*a*) Encontre dois caminhos simples de v_1 a v_6. Um desses caminhos simples é $\alpha = (v_1, v_2, v_4, v_6)$?

(*b*) Encontre todos os ciclos de G que incluem v_3.

(*c*) G é unilateralmente conexo? É fortemente conexo?

(*d*) Encontre a lista de sucessores de cada vértice de G.

(*e*) Há outras fontes em G? Há poços?

(*a*) Um caminho simples é um caminho no qual todos os vértices são distintos. Logo, (v_1, v_5, v_6) e $(v_1, v_2, v_3, v_5, v_6)$ são dois caminhos simples de v_1 a v_6. A sequência não é sequer um caminho, pois a aresta unindo v_4 com v_6 não começa em v_4.

(*b*) Há dois ciclos desse tipo: (v_3, v_1, v_2, v_3) e $(v_3, v_5, v_6, v_1, v_2, v_3)$.

(*c*) G é unilateralmente conexo, uma vez que $(v_1, v_2, v_3, v_5, v_6, v_4)$ é um caminho gerador. G não é fortemente conexo, pois não há caminho gerador fechado.

(*d*) Adicione o vértice v à lista de sucessores $\text{succ}(u)$ de u para cada aresta (u, v) de G. Isso nos leva a:

$$\text{succ}(v_1) = [v_2, v_5], \quad \text{succ}(v_2) = [v_3, v_4], \quad \text{succ}(v_3) = [v_1, v_5]$$
$$\text{succ}(v_4) = \varnothing \quad \text{succ}(v_5) = [v_6], \quad \text{succ}(v_6) = [v_1, v_4]$$

(Como esperado, o número de sucessores é 9, que é a quantia de arestas.)

(*e*) Não há fontes, pois todo vértice é o ponto terminal de alguma aresta. Apenas v_4 é um poço, uma vez que nenhuma aresta começa em v_4, isto é, $\text{succ}(v_4) = \varnothing$, o conjunto vazio.

9.4 Seja G o grafo orientado com conjunto de vértices $V(G) = \{a, b, c, d, e, f, g\}$ e conjunto de arestas.

$$E(G) = \{(a, a), (b, e), (a, e), (e, b), (g, c), (a, e), (d, f), (d, b), (g, g)\}$$

(*a*) Identifique quaisquer laços ou arestas paralelas.

(*b*) Há quaisquer fontes em G?

(*c*) Há poços em G?

(*d*) Encontre o subgrafo H de G determinado pelo conjunto de vértices $V' = \{a, b, c, d\}$.

(*a*) Um laço é uma aresta com os mesmos pontos inicial e final, logo, (a, a) e (g, g) são laços. Duas arestas são paralelas se têm o mesmo ponto inicial e o mesmo ponto terminal. Assim, (a, e) e (a, e) são arestas paralelas.

(*b*) O vértice d é uma fonte, pois nenhuma aresta termina em d, isto é, d não surge como o segundo elemento em qualquer aresta. Não há outras fontes.

(*c*) Ambos c e f são poços, uma vez que nenhuma aresta começa em c ou f, ou seja, nem c, nem f aparecem como o primeiro elemento em qualquer aresta. Não há outros poços.

(*d*) Seja E' o conjunto de todas as arestas de G cujos pontos terminais estão em $V' = \{a, b, c, d\}$. Isso nos conduz a $E' = \{(a, a), (d, b)\}$. Então, $H = H(V', E')$.

Árvores enraizadas, árvores ordenadas com raiz

9.5 Seja T a árvore enraizada na Fig. 9-22.

(*a*) Identifique o caminho α da raiz R para cada um dos seguintes vértices, e determine o nível n do vértice: (i) H; (ii) F; (iii) M.

(*b*) Encontre os irmãos de E.

(*c*) Encontre as folhas de T.

(*a*) Liste os vértices enquanto procede, ao longo da árvore, de R para o vértice. O número de vértices, excluindo R, é o número do nível.

$$\text{(i) } \alpha = (R, A, C, H), n = 3; \text{ (ii) } \alpha = (R, B, F), n = 2; \text{ (iii) } \alpha = (R, B, G, L, M), n = 4.$$

(*b*) Os irmãos de E são F e G, uma vez que todos eles têm a mesma origem B.

(*c*) As folhas são vértices sem filhos, ou seja, H, D, I, J, K, M, N.

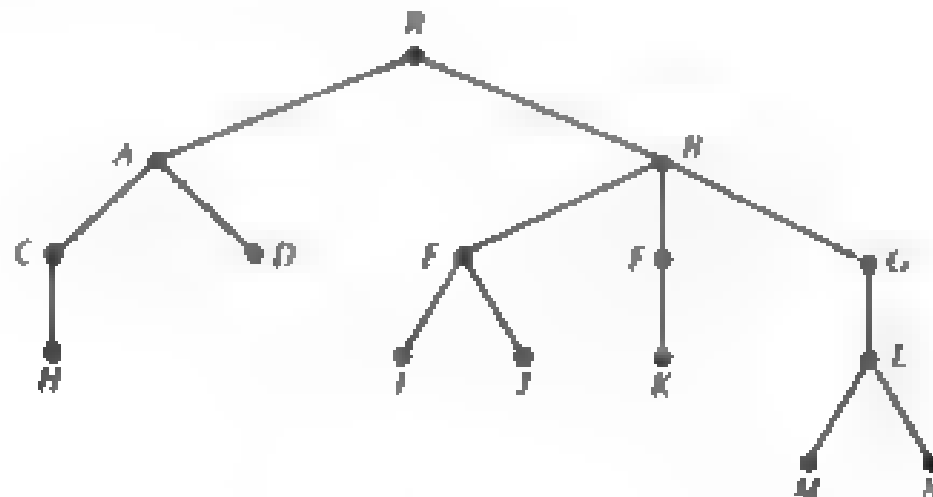



Figura 9-22

9.6 Seja T a árvore orientada enraizada, na Fig. 9-23, cujos vértices são rotulados usando o sistema universal de nomeação. Encontre a ordem lexicográfica dos nomes da árvore T.

Uma árvore orientada T com raiz geralmente é esboçada, de modo que as arestas são ordenadas da esquerda para a direita, como na Fig. 9-23. A ordem lexicográfica pode ser obtida a partir do ramo mais à esquerda, em seguida, o segundo ramo da esquerda, e assim por diante.

A partir do ramo mais à esquerda de T, obtemos:

$$0, \quad 1, \quad 1.1, \quad 1.1.1$$

O próximo ramo é 1.2, 1.2.1, 1.2.1.1, e assim adicionamos esse ramo à lista, para obter

$$0, \quad 1, \quad 1.1, \quad 1.1.1, \quad 1.2, \quad 1.2.1, \quad 1.2.1.1$$

Continuando da mesma maneira, finalmente conseguimos

$$0, \quad 1, \quad 1.1, \quad 1.1.1, \quad 1.2, \quad 1.2.1, \quad 1.2.1.1, \quad 1.2.2, \quad 1.3, \quad 2, \quad 2.1, \quad 2.2.1$$

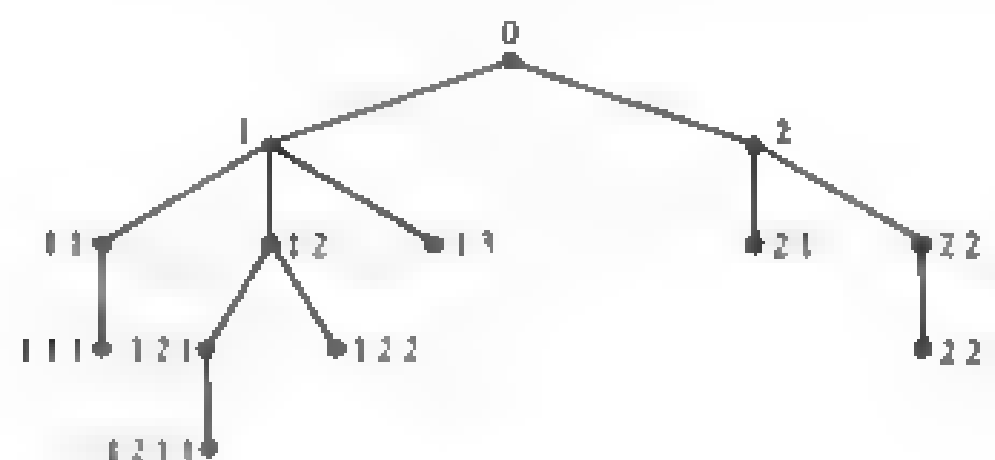



Figura 9-23

Representação sequencial de grafos

9.7 Considere o grafo G na Fig. 9-21(*a*) e suponha que os vértices são armazenados na memória na forma da sequência:

$$\text{DATA: } X, Y, Z, W$$

(*a*) Encontre a matriz de adjacência A do grafo G e as potências A^2, A^3 e A^4

(*b*) Encontre a matriz de caminhos P de G, usando as potências de A. É G fortemente conexo?

(a) Os vértices são normalmente ordenados de acordo com a maneira em que eles aparecem na memória; ou seja, assumimos que $v_1 = X$, $v_2 = Y$, $v_3 = Z$, $v_4 = W$. A matriz de adjacência $A = [a_{ij}]$ é obtida, fazendo $a_{ij} = 1$, se existir uma aresta de v_i a v_j e 0, no caso contrário. A matriz A e suas potências são as que se seguem.

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad A^2 = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 0 & 2 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

(*b*) Como G tem 4 vértices, precisamos encontrar apenas a matriz $B_4 = A + A^2 + A^3 + A^4$ e, em seguida, a matriz de caminhos $P = [p_{ij}]$ é obtida, fazendo $p_{ij} = 1$, quando existir uma entrada não nula na matriz B_4 e 0, no caso contrário. As matrizes B_4 e P são as que se seguem.

$$B_4 = \begin{bmatrix} 0 & 5 & 6 & 8 \\ 0 & 1 & 2 & 3 \\ 0 & 3 & 3 & 5 \\ 0 & 2 & 3 & 5 \end{bmatrix} \quad \text{e} \quad P = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

A matriz de caminhos P mostra que não há caminho a partir de qualquer nó até v_1. Logo, G não é fortemente conexa.

9.8 Considere a matriz de adjacência A do grafo G na Fig. 9-19(*a*) obtida no Problema 9.7. Determine a matriz de caminhos P de G, usando o algoritmo de Warshall em vez das potências de A.

Primeiro, fazemos $P_0 = A$. A seguir, P_1, P_2, P_3 e P_4 são obtidas recursivamente, fazendo

$$P_k[i, j] = P_{k-1}[i, j] \vee (P_{k-1}[i, k] \wedge P_{k-1}[k, j])$$

onde $P_k[i, j]$ denota a entrada ij na matriz P_k. Isto é, fazendo

$$P_k[i, j] = 1 \text{ se } P_{k-1}[i, j] = 1 \text{ ou se ambos } P_{k-1}[i, k] = 1 \text{ e } P_{k-1}[k, j] = 1$$

Então as matrizes P_1, P_2, P_3 e P_4 são as que se seguem.

$$P_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad P_3 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & \end{bmatrix}, \quad P_4 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Observe que $P_1 = P_2 = A$. As mudanças em P_3 ocorrem pelos seguintes motivos:

$$P_3[4, 2] = 1, \text{ porque } P_2[4, 3] = 1 \text{ e } P_2[3, 2] = 1$$
$$P_3[4, 4] = 1, \text{ porque } P_2[4, 3] = 1 \text{ e } P_2[3, 4] = 1$$

9.9 Desenhe uma imagem do grafo ponderado G que é mantido na memória pelo seguinte array DATA de vértices e pela matriz W de pesos:

$$\text{DATA: } X, Y, S, T; \quad W = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 5 & 0 & 1 & 7 \\ 2 & 0 & 0 & 4 \\ 0 & 6 & 8 & 0 \end{bmatrix}$$

A imagem aparece na Fig. 9-24(*a*). Os vértices são rotulados pelas entradas em DATA.

Assumindo $v_1 = X$, $v_2 = Y$, $v_3 = S$, $v_4 = T$, a ordem dos vértices aparece no array DATA, desenhamos uma aresta de v_i a v_j com peso w_{ij} quando $w_{ij} \neq 0$.

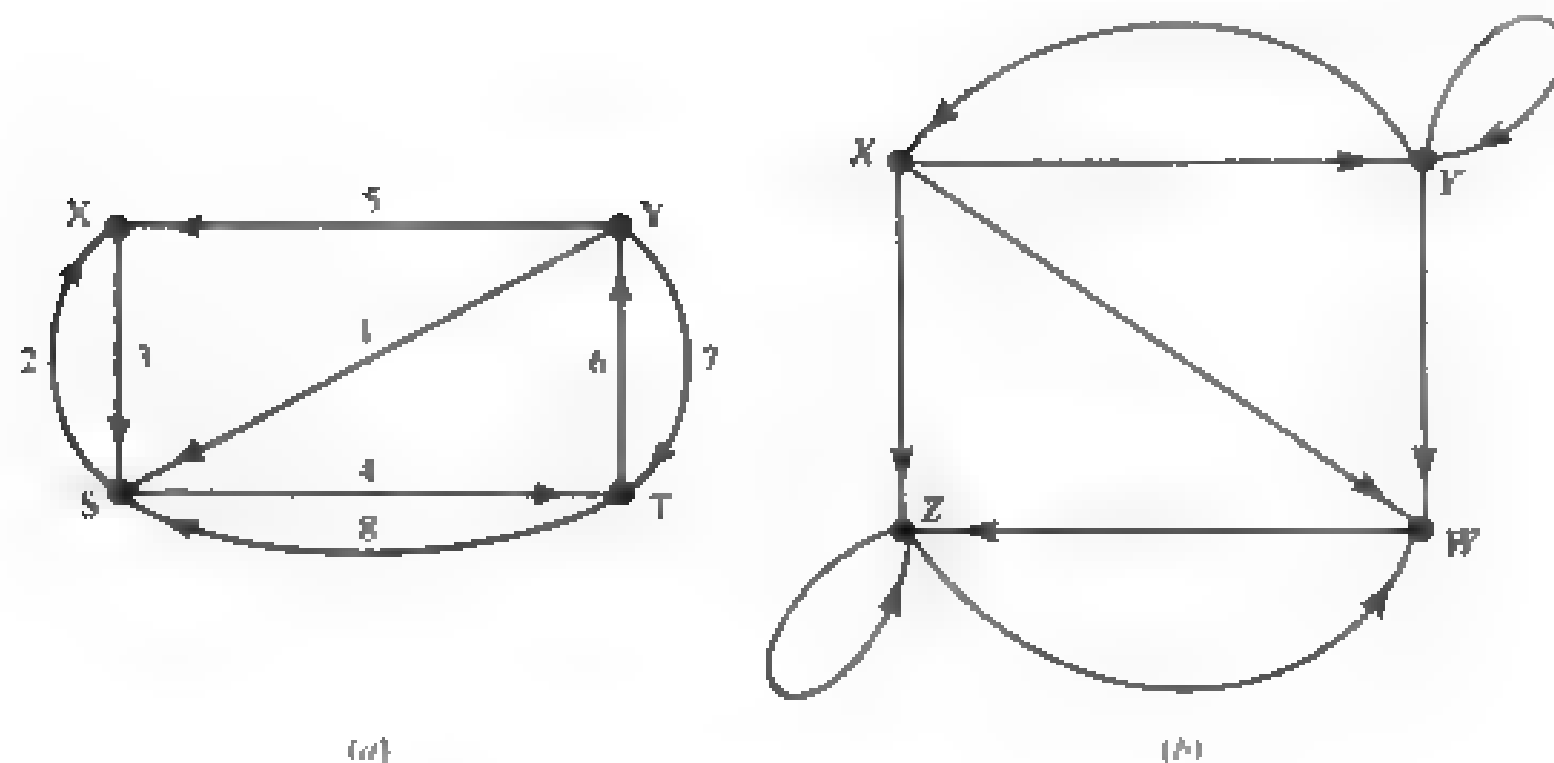



Figura 9-24

Representação ligada de grafos

9.10 Seja G o grafo apresentado pela seguinte tabela:

$$G = [X : Y, Z, W;\ Y : X, Y, W;\ Z : Z, W;\ W : Z]$$

(a) Encontre a quantia de vértices e arestas de G.

(b) Desenhe o grafo G.

(c) Há quaisquer fontes ou poços?

(a) A tabela nos diz que existem quatro vértices, X, Y, Z, W. Os graus de saída dos vértices são 3, 3, 2, 1, respectivamente. Logo, há $3 + 3 + 2 + 1 = 9$ arestas.

(b) Usando as listas de adjacência, esboce o grafo na Fig. 9-24(b).

(c) Nenhum vértice tem grau de saída nulo; logo, não há poços. Além disso, nenhum vértice tem grau de entrada nulo, ou seja, cada vértice é um sucessor; logo, não há fontes.

9.11 Um grafo ponderado G com seis vértices $A, B, \ldots, F$ é armazenado na memória, usando-se uma representação ligada com um arquivo de vértices e um arquivo de arestas, como na Fig. 9-25(a).

Arquivo de vértices

START [3]

	1	2	3	4	5	6	7	8
VERTEX	D		B	F	A		C	E
NEXT-V	7		1	5	0		8	4
PTR	9		3	0	6		10	1

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10
BEG-V	8	5	3		5	5	3			7
END-V	1	4	7		3	1	1		8	8
NEXT-E	0	5	7		0	2	0		0	0
PESO	3	4	2		6	3	1		7	5

(a)

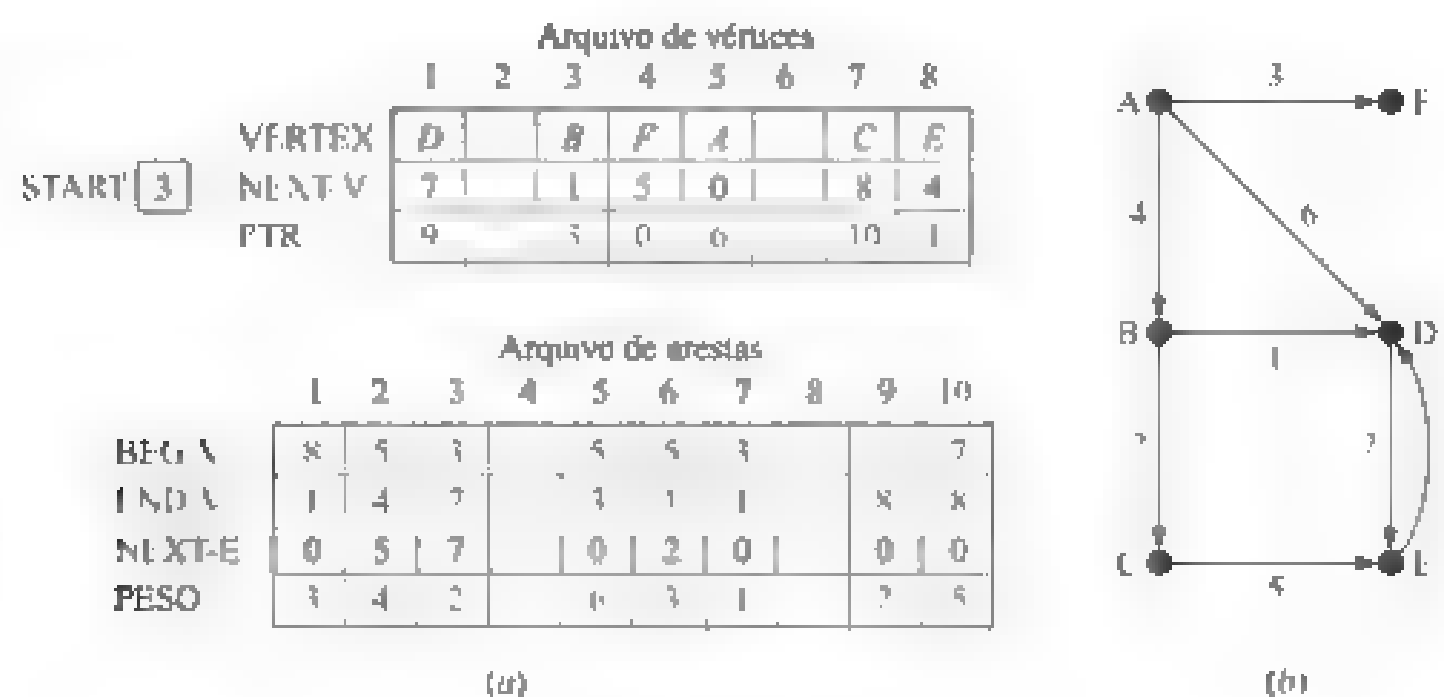



Figura 9-25

(a) Liste os vértices na ordem em que eles aparecem na memória.

(b) Determine a lista de sucessores succ(v) de cada vértice v.

(c) Desenhe o grafo G.

(*a*) Como START = 3, a lista começa com o vértice B. A seguir, NEXT-V nos diz para ir a 1(D), então 7(C), seguido de 8(E), depois, 4(F) e, por último, para 5(A); ou seja,

$$B, \quad D, \quad C, \quad E, \quad F, \quad A$$

(*b*) Aqui succ(A) = [1(D), 4(F), 3(B)] = [D, F, B]. Especificamente, PTR[5(A)] = 6 e END-V[6] = 1(D) nos dizem que succ(A) começa com D. Então NEXT-E[6] = 2 e END-V[2] = 4(F) nos dizem que F é o próximo vértice em succ(A). Em seguida, NEXT-E[2] = 5 e END-V[5] = 3(B) nos dizem que B é o próximo vértice em succ(A). Contudo, NEXT-E[5] = 0 nos diz que não há mais sucessores de A. Analogamente,

$$\text{succ}(B) = [C, D], \quad \text{succ}(C) = [E], \quad \text{succ}(D) = [E], \quad \text{succ}(E) = [D]$$

Além disso, succ(F) = ∅, uma vez que PTR[4(F)] = 0. Em outras palavras,

$$G = [A{:}D, F, B; \quad B{:}C, D; \quad C{:}E; \quad D{:}E; \quad E{:}D; \quad F{:}\varnothing]$$

(*c*) Use as listas de sucessores obtidas em (b) e os pesos das arestas no Arquivo de Arestas da Fig. 9-25(*a*) para esboçar o grafo na Fig. 9-25(*b*).

9.12 **Suponha que a Friendly Airways tem nove voos diários como se segue:**

103 de Atlanta para Houston	203 de Boston para Denver	305 de Chicago para Miami
106 de Houston para Atlanta	204 de Denver para Boston	308 de Miami para Boston
201 de Boston para Chicago	301 de Denver para Reno	401 de Reno para Chicago

Descreva os dados por meio de um grafo orientado rotulado G.

Os dados são descritos pelo grafo na Fig. 9-26(*a*) (onde os números dos voos foram omitidos por conveniência notacional).

(*a*)

Arquivo de vértices

	1	2	3	4	5	6	7	8
CIDADE	A	B	C	D	H	M	R	
PTR	1	3	7	5	2	8	9	

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10
NÚMERO	103	06	201	203	204	301	305	308	401	
ORIGEM	1	5	2	2	4	4	3	6	7	
DESTINO	5	1	3	4	2	7	6	2	3	
NEXT-E	0	0	4	0	6	0	0	0	0	

(*b*)

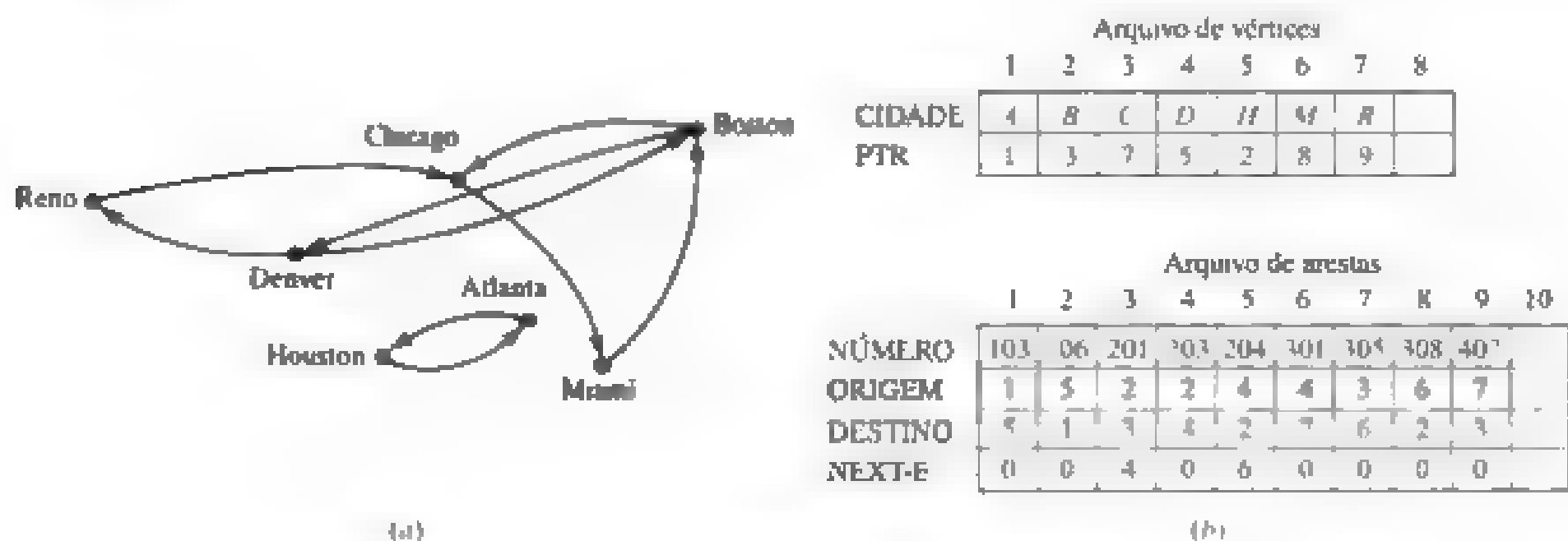



Figura 9-26

9.13 **Descreva como o grafo no Problema 9.12 pode aparecer na memória, usando uma representação ligada, onde as cidades e os voos aparecem em arrays lineares ordenados.**

Ver Fig. 9-26(*b*) (onde A, B, ... denotam, respectivamente, Atlanta, Boston, ...). Não há necessidade para uma variável START, pois as cidades formam um array e não uma lista ligada. Também empregamos ORIGEM e DESTINO no lugar de BEG-V e END-V.

9.14 **Claramente, os dados no Problema 9.12 podem ser armazenados de maneira eficiente em um arquivo onde cada registro contém apenas três campos:**

Número do Voo, Cidade de Origem, Cidade de Destino

Contudo, quando há muitos, muitos voos, tal representação não responde facilmente às seguintes questões naturais:

(i) Há algum voo direto da cidade X para a cidade Y?

(ii) É possível voar da cidade X para a cidade Y?

(iii) Qual é a rota mais direta (com número mínimo de paradas) da cidade X para a cidade Y?

Mostre como a resposta, digamos, ao item (ii), pode ser mais prontamente disponível se os dados são armazenados na memória, usando a representação ligada do grafo, como na Fig. 9-26(b).

Uma maneira de responder (ii) é usando o algoritmo de busca em largura ou busca em profundidade para decidir se a cidade Y é alcançável a partir da cidade X. Tais algoritmos exigem as listas de adjacência, que podem ser facilmente obtidas a partir da representação ligada de um grafo, mas não da representação acima, a qual emprega apenas três campos.

Problemas variados

9.15 Seja $A = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ a matriz de adjacência de um multigrafo G. Esboce uma imagem de G

Como A é uma matriz 4×4, G tem quatro vértices, v_1, v_2, v_3, v_4. Para cada entrada a_{ij} de A, desenhe a_{ij} arcos (arestas orientadas) do vértice v_i ao vértice v_j, para obter o grafo na Fig. 9-27(a).

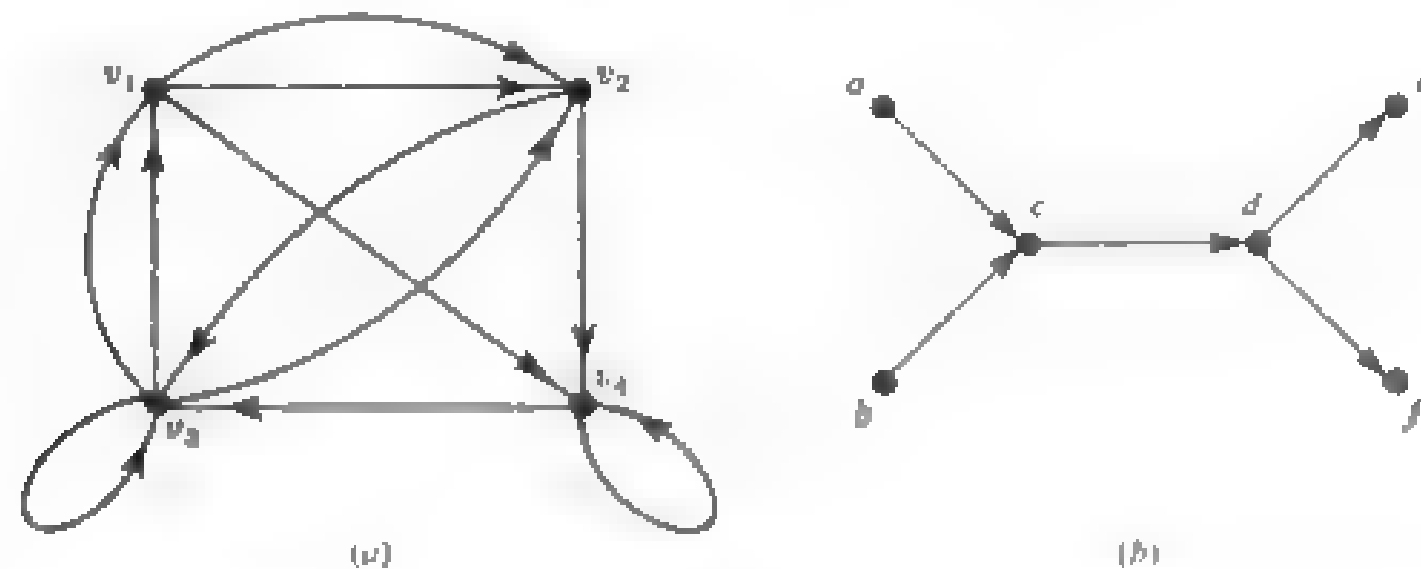



Figura 9-27

9.16 Seja S o grafo livre de ciclos na Fig. 9-27(b). Encontre todas as ordenações topológicas de S.

Existem quatro possíveis ordenações topológicas de S. Especificamente, cada ordenação T deve começar com a ou b, deve terminar com e ou f, e c e d devem ser o terceiro e o quarto elementos, respectivamente. As quatro ordenações são as que se seguem:

$$T_1 = [a, b, c, d, e, f], \quad T_2 = [b, a, c, d, e, f],$$
$$T_3 = [a, b, c, d, f, e], \quad T_4 = [b, a, c, d, f, e].$$

9.17 Demonstre a Proposição 9.4: Seja A a matriz de adjacência G de um grafo G. Então $a_K[i, j]$, a entrada ij da matriz A^K, fornece o número de caminhos de comprimento K de v_i a v_j.

A demonstração é por indução sobre K. Um caminho de comprimento 1 de v_i a v_j é precisamente uma aresta (v_i, v_j). Pela definição da matriz de adjacência A, $a_1[i, j] = a_{ij}$ fornece o número de arestas de v_i a v_j. Logo, a proposição é verdadeira para $K = 1$.

Suponha que $K > 1$. (Assuma que G tem m nós.) Como $A^K = A^{K-1}A$,

$$a_K[i, j] = \sum_{s=1}^{m} a_{K-1}[i, s]\, a_1[s, j]$$

Por indução, $a_{K-1}[i, s]$ dá o número de caminhos de comprimento $K-1$ de v_i a v_s, e $a_1[s, j]$ fornece o número de caminhos de comprimento 1 de v_s a v_j. Portanto, $a_{K-1}[i, s]a_1[s, j]$ dá o número de caminhos de comprimento K de v_i a v_j, onde v_s é o penúltimo vértice. Assim, todos os caminhos de comprimento K de v_i a v_j podem ser obtidos, somando os produtos $a_{K-1}[i, s]a_1[s, j]$ para todo s. Consequentemente, $a_K[i, j]$ é o número de caminhos de comprimento K de v_i a v_j. Assim, a proposição é provada.

Problemas Complementares

Terminologia de grafos

9.18 Considere o grafo G na Fig. 9-28(a).

(a) Encontre o grau de entrada e o grau de saída de cada vértice.

(b) Há quaisquer fontes ou poços?

(c) Determine todos os caminhos simples de v_1 a v_4.

(d) Encontre todos os ciclos de G.

(e) Determine todos os caminhos de comprimento menor ou igual a 3 de v_1 a v_3.

(f) G é unilateral ou fortemente conexo?

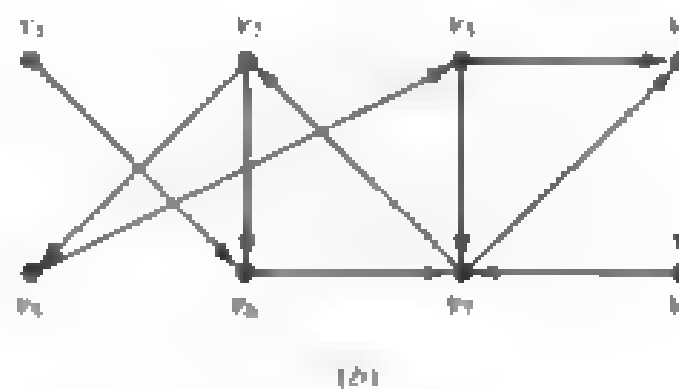
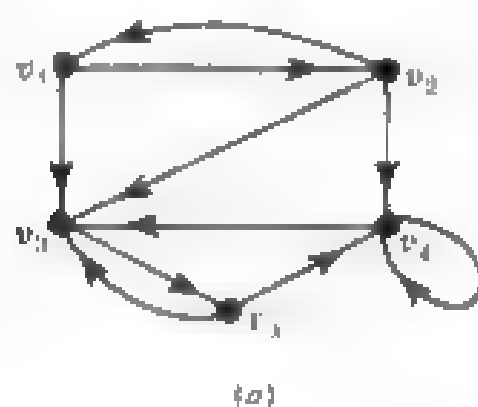



Figura 9-28

9.19 Considere o grafo G na Fig. 9-28(b).

(a) Há quaisquer fontes ou poços?

(b) Encontre todos os caminhos simples de v_1 a v_4.

(c) Encontre um caminho não simples de v_1 a v_4.

(d) Encontre todos os ciclos de G que incluem v_4.

9.20 Considere o grafo G na Fig. 9-28(b).

(a) Determine: succ(v_1), succ(v_3), succ(v_5), succ(v_7).

(b) Encontre o subgrafo H de G gerado por: (i) $\{v_1, v_3, v_5, v_6\}$, (ii) $\{v_2, v_3, v_6, v_7\}$.

9.21 Seja G o grafo com conjunto de vértices $V(G) = \{A, B, C, D, E\}$ e conjunto de arestas

$$E(G) = \{(A, D), (B, C), (C, E), (D, B), (D, D), (D, E), (E, A)\}$$

(a) Expresse G por sua tabela de adjacência.

(b) G tem laços ou arestas paralelas?

(c) Encontre todos os caminhos simples de D a E.

(d) Encontre todos os ciclos de G

(e) G é unilateral ou fortemente conexo?

(f) Encontre o número de subgrafos de G com vértices C, D e E.

(g) Encontre o subgrafo H de G gerado por C, D e E.

9.22 Seja G o grafo com conjunto de vértices $V(G) = \{a, b, c, d, e\}$ e as seguintes listas de sucessores:

$$\text{succ}(a) = \{b, c\},\ \text{succ}(b) = \varnothing,\ \text{succ}(c) = \{d, e\},\ \text{succ}(d) = \{a, b, e\},\ \text{succ}(e) = \varnothing$$

(a) Liste as arestas de G. (b) G é fraca, unilateral ou fortemente conexo?

9.23 Seja G o grafo na Fig. 9-29(a).

(a) Expresse G por meio de sua tabela de adjacência.

(b) G tem quaisquer fontes ou poços?

(c) Determine todos os caminhos simples de A a E.

(d) Encontre todos os ciclos de G.

(e) Encontre um caminho gerador de G.

(f) G é fortemente conexo?

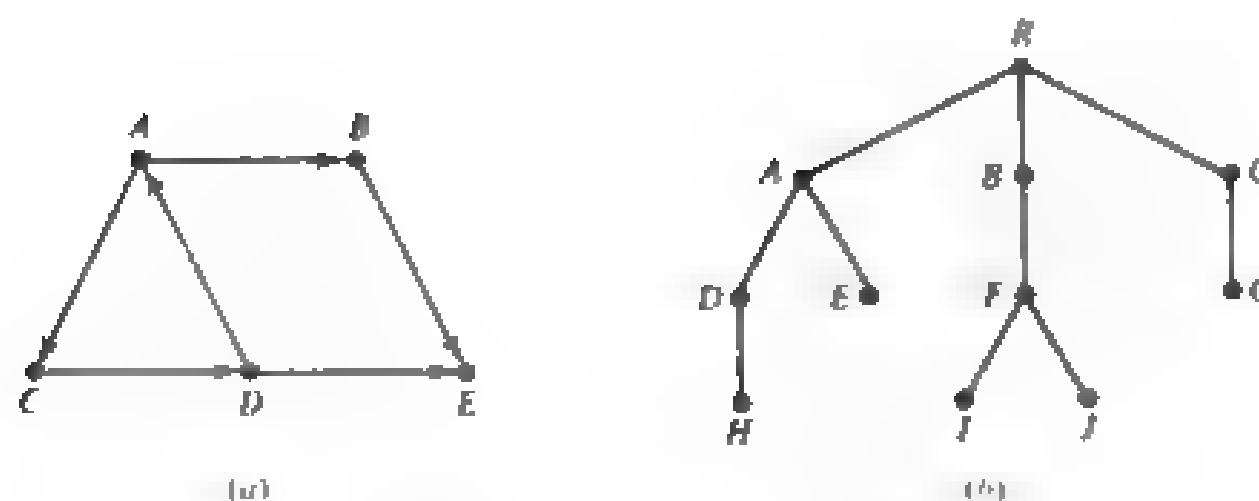



Figura 9-29

Árvores enraizadas, árvores ordenadas com raiz

9.24 Seja T a árvore enraizada na Fig. 9-29(b).

(a) Identifique o caminho α da raiz R a cada um dos seguintes vértices e encontre o nível de cada um. (i) D; (ii) J; (iii) G.

(b) Encontre as folhas de T.

(c) Assumindo que T é uma árvore ordenada, determine a nomeação universal de cada folha de T.

9.25 Os nomes a seguir estão em ordem aleatória.

2.1.1, 3.1, 2.1, 1, 2.2.1 2, 0, 3.2, 2.2, 1.1, 2, 3.1.1, 2.2.1, 3, 2.2.1.1

(a) Coloque os nomes em ordem lexicográfica.

(b) Desenhe a árvore enraizada correspondente.

Representação sequencial de grafos

9.26 Seja G o grafo na Fig. 9-30(a).

(a) Encontre a matriz de adjacência A e a matriz de caminhos P para G.

(b) Para todo $k > 0$, determine n_k, onde n_k denota o número de caminhos de comprimento k de v_1 a v_4.

(c) G é fraca, unilateral ou fortemente conexo?

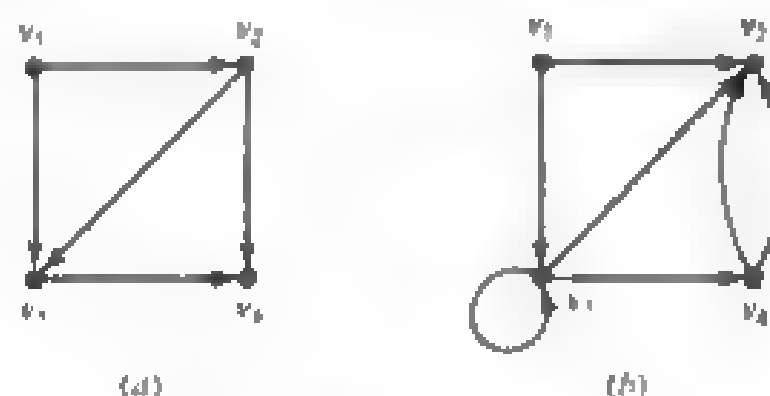



Figura 9-30

9.27 Repita o Problema 9.26 para o grafo G na Fig. 9-30(b).

9.28 Seja P a matriz de caminhos para um grafo G. Descreva P quando G é: (a) fortemente conexo; (b) unilateralmente conexo.

9.29 Seja G o grafo na Fig. 9-31(a), onde os vértices são mantidos na memória pelo array DATA: X, Y, Z, S, T. (a) Encontre a matriz de adjacência A e a matriz de caminhos P de G. (b) Determine todos os ciclos de G. (c) G é unilateralmente conexo? É fortemente conexo?

9.30 Seja G o grafo ponderado na Fig. 9-31(b), onde os vértices são mantidos na memória pelo array DATA: X, Y, S, T.

(a) Encontre a matriz W de pesos de G.

(b) Encontre a matriz Q de caminhos mais curtos, usando o algoritmo de Warshall.

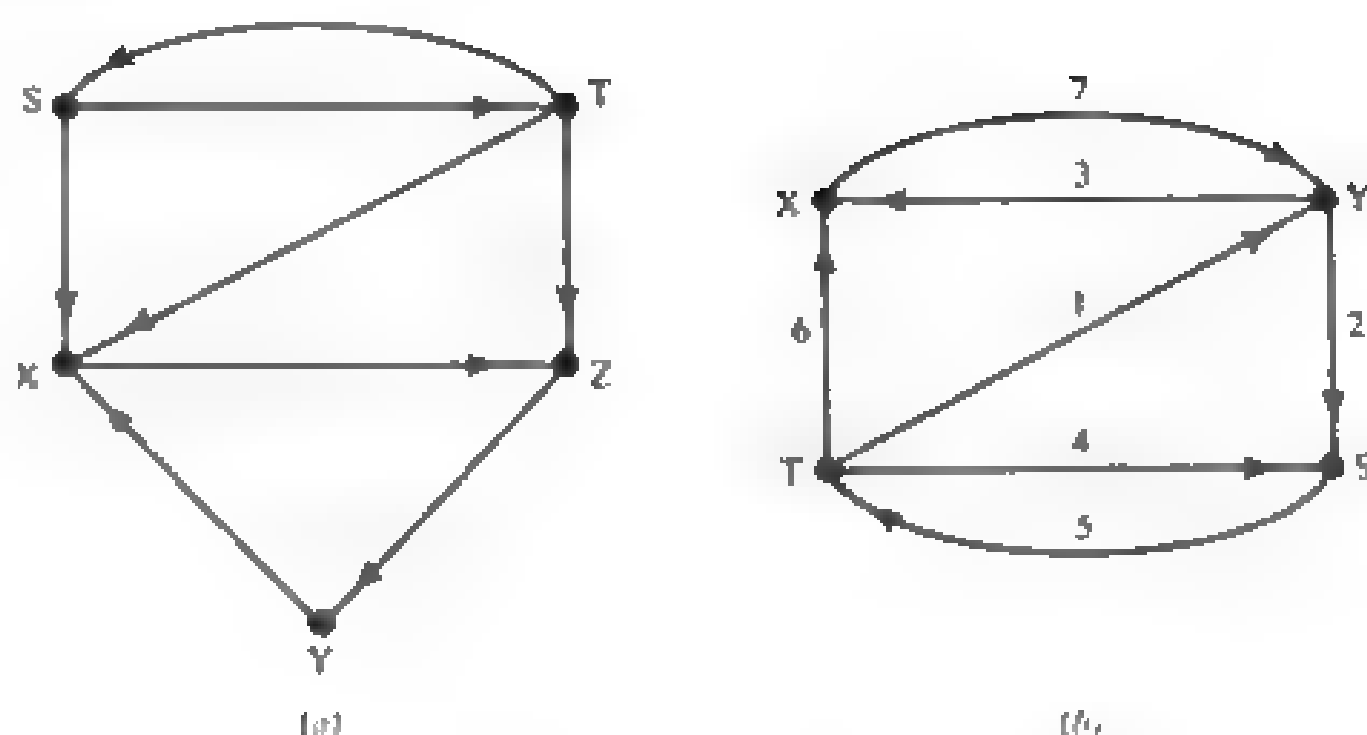



Figura 9-31

Representação ligada de grafos

9.31 Um grafo ponderado G com seis vértices $A, B, \ldots, F$, é armazenado na memória, usando uma representação ligada com um arquivo de vértices e um de arestas, como na Fig. 9-32.

(a) Liste os vértices na ordem em que eles aparecem na memória.

(b) Encontre a lista de sucessores succ(v) de cada vértice v de G

(c) Desenhe uma imagem de G.

Arquivo de vértices

START [7]

		2	3	4	5	6	7	8
VERTEX	D		B	F	A		C	E
NEXT-V	3		8		0		4	5
PTR	7		5	9	2		1	0

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10	11	12
BEG-V	5	5	7		3	7	1		4	1	4	7
END-V	8	7	5		1	1	5		8	4	3	8
NEXT-E	0	1	12		0	0	10		11	0	0	6
PESO	5	2	1		3	2	4		1	3	4	1

Figura 9-32

9.32 Seja G o grafo apresentado pela tabela $G = [A{:}B, C;\ B{:}C, D;\ C{:}C;\ D{:}B;\ E{:}\varnothing]$.

(a) Encontre o número de vértices e de arestas em G.

(b) Esboce uma imagem de G.

(c) Há quaisquer fontes ou poços?

(d) G é fraca, unilateral ou fortemente conexo?

9.33 Repita o Problema 9.32 para a tabela $G = [A{:}D;\ B{:}C;\ C{:}E;\ D{:}B, D, E;\ E{:}A]$.

9.34 Repita o Problema 9.32 para a tabela $G = [A{:}B, C, D, K;\ B{:}J;\ C{:}\varnothing;\ D{:}\varnothing;\ J{:}B, D, L;\ K{:}D, L;\ L{:}D]$

9.35 Suponha que a Friendly Airways tem oito voos diários atendendo as sete cidades: Atlanta, Boston, Chicago, Denver, Houston, Philadelphia, Washington. Suponha que os dados dos voos são armazenados na memória como na Fig. 9-33, ou seja, usando uma representação ligada na qual as cidades e os voos aparecem em arrays lineares ordenados. Esboce um grafo orientado G rotulado, descrevendo os dados.

Arquivo de vértices

	1	2	3	4	5	6	7	8
CIDADE	*A*	*B*	*C*	*D*	*H*	*P*	*W*	
PTR	1	2	3	8	9	5	7	

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10
NUMERO DO VOO	101	102	201	202	203	301	302	401	402	
ORIGEM	1	2	3	1	6	6	7	4	5	
DESTINO	2	3	6	7	3	1	6	5	4	
NEXT-E	4	0	0	0	6	0	0	0	0	

Figura 9-33

9.36 Utilizando os dados da Fig. 9-33, escreva um procedimento com entradas CIDADE X e CIDADE Y que encontre o número do voo de um trajeto direto da cidade X para a cidade Y, se existir. Teste o procedimento, usando:

(a) X = Atlanta, Y = Philadelphia; (c) X = Houston, Y = Chicago;

(b) X = Philadelphia, Y = Atlanta; (d) X = Washington, Y = Chicago.

9.37 Utilizando os dados da Fig. 9-33, escreva um procedimento com entradas CIDADE X e CIDADE Y que encontre a rota mais direta (numero mínimo de paradas) da cidade X para a cidade Y, se existir. Teste o procedimento usando as entradas do Problema 9.36.

Problemas variados

9.38 Use o algoritmo de poda para encontrar o caminho mais curto de s a t na Fig. 9-34.

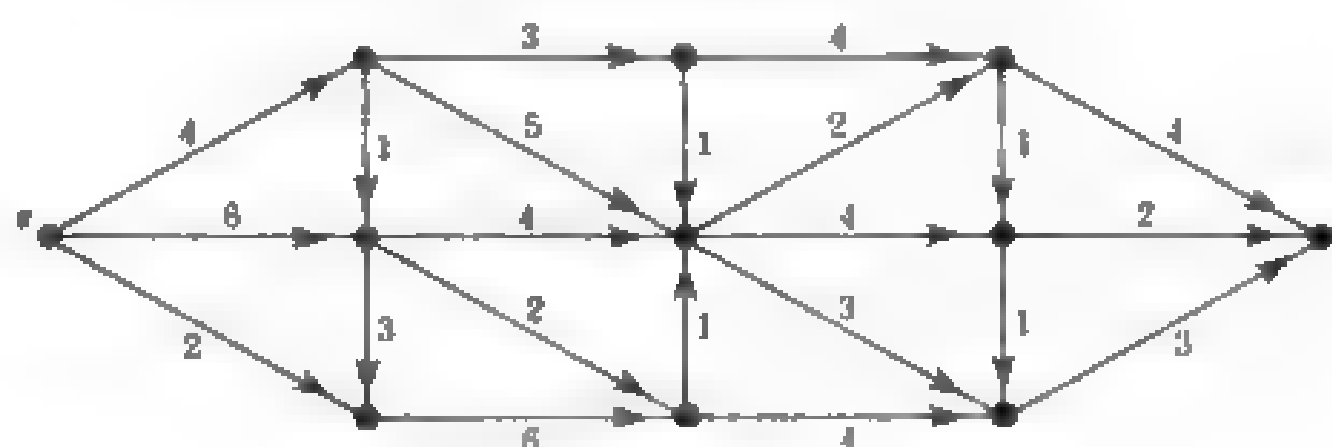



Figura 9-34

9.39 Encontre uma ordenação topológica T de cada um dos grafos a seguir:

(a) $G = [A: Z;\ \ B: T;\ \ C: B;\ \ D: \varnothing;\ \ X: D;\ \ Y: X;\ \ Z: B, X;\ \ S: C, Z;\ \ T: \varnothing]$

(b) $G = [A: X, Z;\ \ B: A;\ \ C: S, T;\ \ D: Y;\ \ X: S, T;\ \ Y: B;\ \ Z: \varnothing;\ \ S: Y;\ \ T: \varnothing]$

(c) $G = [A: C, S;\ \ B: T, Z;\ \ C: \varnothing;\ \ D: Z;\ \ X: A;\ \ Y: A;\ \ Z: X, Y;\ \ S: \varnothing;\ \ T: Y]$

9.40 Desenhe um grafo rotulado G que representa a situação a seguir. Três irmãs, Bárbara, Rose e Susana, telefonam regularmente para a mãe Gertrude, apesar de que Gertrude telefona apenas para Rose. Susana não liga para Rose, apesar de Rose continuar telefonando para Susana. Bárbara e Susana telefonam uma para a outra, e Bárbara e Rose também ligam uma para a outra.

9.41 Seja R a relação (grafo orientado) sobre $V = \{2, 3, 4, 9, 15\}$ definida por "x é menor do que e primo relativo de y." (a) Desenhe o diagrama do grafo R. (b) R é fracamente conexo? Unilateralmente conexo? Fortemente conexo?

9.42 Um grafo orientado G é completo se, para cada par de vértices distintos u e v, (u, v) ou (v, u) é um arco. Mostre que um grafo orientado completo finito G tem um caminho que inclui todos os vértices. (Isso obviamente vale para grafos completos não orientados.) Assim, G é unilateralmente conexo.

9.43 Suponha que um grafo G é inserido em um computador por meio de um inteiro M, representando os vértices 1, 2, ..., M, e uma lista de N pares ordenados de inteiros, representando as arestas de G. Escreva um procedimento para cada um dos itens a seguir:

(a) Encontre a matriz de adjacência A $M \times M$ do grafo G.

(b) Use A e o algoritmo de Warshall para encontrar a matriz de caminhos P de G.

Teste o procedimento acima, utilizando os seguintes dados.

(i) $M = 5$; $N = 8$, (3, 4), (5, 3), (2, 4), (1, 5), (3, 2), (4, 2), (3, 1), (5, 1)

(ii) $M = 6$; $N = 10$; (1, 6), (2, 1), (2, 3), (3, 5), (4, 5), (4, 2), (2, 6), (5, 3), (4, 3), (6, 4)

9.44 Suponha que um grafo G é inserido em um computador por meio de um inteiro M, representando os vértices 1, 2, ..., M, e uma lista de N triplas ordenadas (a_i, b_i, w_i) de inteiros, tais que (a_i, b_i) é uma aresta de G e w_i é seu peso. Escreva um procedimento para cada um dos itens a seguir:

(a) Encontre a matriz ponderada W $M \times M$ do grafo G.

(b) Use W e o algoritmo de Warshall para determinar a matriz Q de caminhos mais curtos entre os vértices de G.

Teste o procedimento acima, usando os seguintes dados:

(i) $M = 4$, $N = 7$; (1, 2, 5), (2, 4, 2), (3, 2, 3), (1, 1, 7), (4, 1, 4), (4, 3, 1)

(ii) $M = 5$; $N = 8$, (3, 5, 3), (4, 1, 2), (5, 2, 2), (1, 5, 5), (1, 3, 1), (2, 4, 1), (3, 4, 4), (5, 4, 4)

9.45 Considere o grafo G na Fig. 9-11. Mostre a sequência de listas de espera em PILHA e a sequência de vértices processados enquanto se realiza uma busca em profundidade (DFS) de G começando nos vértices: (a) B, (b) E, (c) K.

9.46 Considere o grafo na Fig. 9-11. Como no Exemplo 9.11, encontre o caminho mais curto de K a F, usando uma busca em largura de G. Em particular, mostre a sequência de listas de espera em FILA durante a busca.

Respostas dos Problemas Complementares

Notação $M = [R_1, R_2, \ldots, R_n]$ denota uma matriz com linhas $R_1, R_2, \ldots, R_n$.

9.18 (a) graus de entrada: 1, 1, 4, 3, 1; graus de saída: 2, 3, 1, 2, 2.

(b) Nenhum.

(c) (v_1, v_2, v_4), (v_1, v_3, v_5, v_4), $(v_1, v_2, v_3, v_5, v_4)$

(d) (v_3, v_5, v_4, v_3)

(e) (v_1, v_3), (v_1, v_2, v_3), (v_1, v_2, v_4, v_3), (v_1, v_2, v_1, v_3), (v_1, v_3, v_5, v_3)

(f) Unilateralmente, mas não fortemente.

9.19 (a) Fontes: v_1

(b) (v_1, v_6, v_7, v_4), $(v_1, v_6, v_7, v_2, v_5, v_3, v_4)$

(c) $(v_1, v_6, v_7, v_2, v_6, v_7, v_4)$

(d) (v_4, v_8, v_7, v_4), $(v_4, v_8, v_7, v_2, v_5, v_3, v_4)$

9.20 (a) succ(1) = [6], succ(3) = [4, 7], succ(5) = [3], succ(7) = [2, 4].

(b) (i) (1, 6), (5, 3); (ii) (2, 6), (6, 7), (7, 2), (3, 7).

9.21 (a) $G = [A: D; B: C; C: E; D: B, D, E; E: A]$

(b) Laço: (D, D)

(c) (D, E), (D, B, C, E)

(d) (A, D, E, A), (A, D, B, C, E, A)

(e) Unilateralmente e fortemente.

(f) E (g) H têm três arestas. (C, E), (D, E), (D, D). Há $8 = 2^3$ maneiras de escolher algumas das três arestas; e cada escolha corresponde a um subgrafo.

9.22 (a) (a, b), (a, c), (c, d), (c, e), (d, a), (d, b), (d, e)

(b) Como b e e são poços, não há caminho de b a e ou de e a b e, portanto, G não é unilateralmente conexo nem fortemente conexo. G é fracamente conexo, pois cc, a, b, d, e é um semicaminho gerador

9.23 (a) $G = [A: B, C: B: E; C: D; E: \varnothing]$, (b) Poço: E; (c) (A, B, E), (A, C, D, E); (d) (A, C, D, A); (e) $C, D, A, B, E)$; (f) Não.

9.24 (a) (i) (R, A, D), 2; (ii) (R, B, F, J), 3; (iii) (R, C, G), 2.

(b) H, E, I, J, G

(c) H : 1.1.1, E : 1.2, I : 2.1.1, J : 2.1.2, G : 3 1

9.25 (a) 0, 1, 1 1, 2, 2.1, 2.1.1, 2.2, 2.2.1, 2.2.1.1, 2.2.1.2, 3, 3.1, 3.1.1, 3.2. (b) Fig. 9-35(*a*).

9.26 (a) $A = [0, 1, 1, 0; 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0]$, $P = [0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0]$;

(b) 0, 2, 1, 0, 0, . . .; (c) fraca e unilateralmente conexo.

9.27 (a) $A = [0, 1, 1, 0; 0, 0, 0, 0; 0, 1, 1, 1; 0, 2, 0, 0]$, $P = [0, 1, 1, 1; 0, 0, 0, 0; 0, 1, 1, 1, 0, 1, 0, 0]$,

(b) 0, 1, 1, 1, . . ; (c) fraca e unilateralmente conexo.

9.28 Seja $P = [p_{ij}]$. Para $i \neq j$: (a) $p_{ij} \neq 0$; (b) $p_{ij} \neq 0$ ou $p_{ji} \neq 0$.

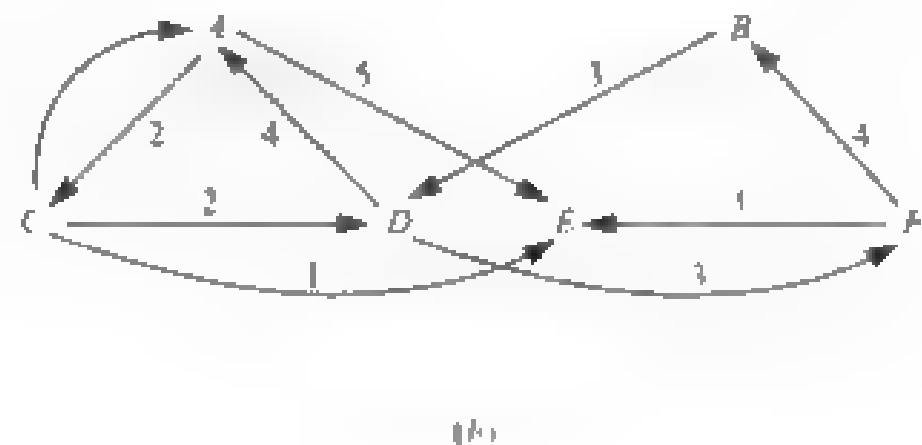
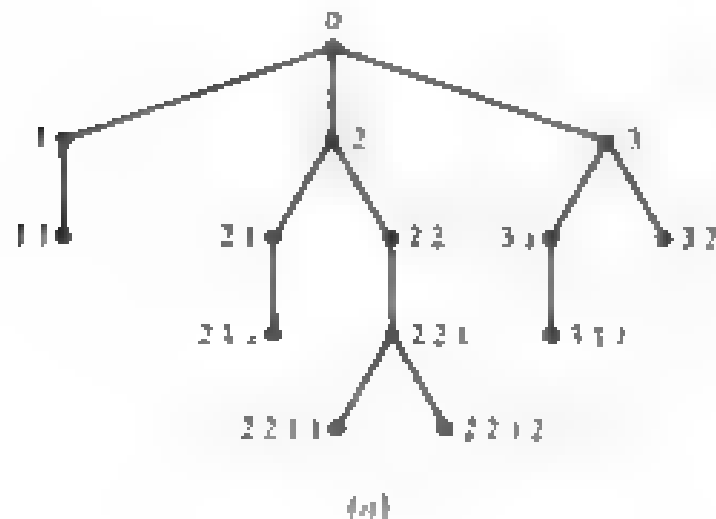



Figura 9-35

9.29 (a) $A = [0, 0, 1, 0, 0; 1, 0, 0, 0, 0; 0, 1, 0, 0, 0; 1, 0, 0, 0, 1, 1, 0, 1, 1, 0]$, $P = [1, 1, 1, 0, 0; 1, 1, 1, 0, 0; 1, 1, 1, 0, 0; 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]$

(b) (X, Z, Y, X); (S, T, S); (c) Unilateralmente conexo.

9.30 (a) $A = [0, 7, 0, 0; 3, 0, 2, 0; 0, 0, 0, 5; 6, 1, 4, 0]$

(b) $Q = [XYX, XY, XYS, XYST; YX, YSTY, YS, YST; STYX, STY, STYS, ST; TX, TY, TYS, TYST]$

9.31 (a) C, F, D, B, E, A, (b) $[A : C, E; B : D; C : D, E, A, D : A, F; E : \varnothing, F : B, E]$; (c) Ver Fig. 9-35(*b*).

9.32 (a) 5, 6; (b) fonte: A; (c) ver Fig. 9-36(*a*); nenhum.

9.33 (a) 5, 1; (b) nenhum; (c) ver Fig. 9-36(*b*); (d) os três.

9.34 (a) 7, 11, (b) fonte: A, poços: C, D; (c) ver Fig. 9-36(*c*); (d) apenas fracamente.

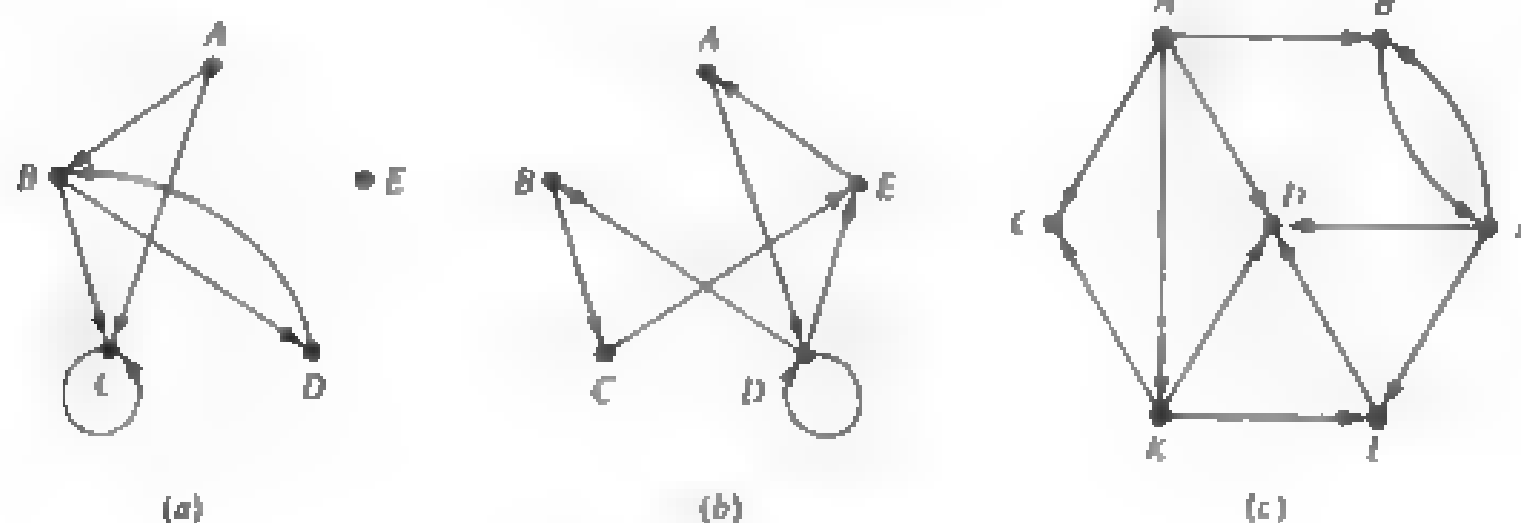



Figura 9-36

9.35 Ver Fig. 9-37

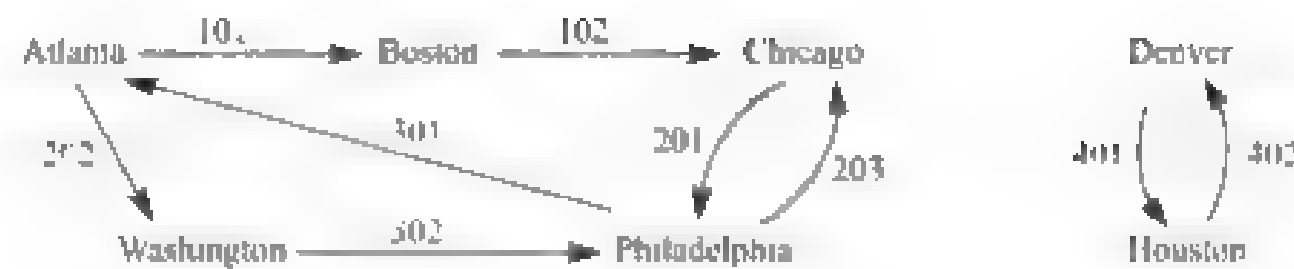



Figura 9-37

9.36 (a) Não; (b) Sim; (c) Não; (d) Não.

9.37 (a) *AWP*; (b) *PA*; (c) nenhum; (d) *WPC*.

9.38 (*s*, 4, 1, 2, 1, 2, 1, 2, *t*)

9.39 ***Sugestão*:** Primeiro desenhe o grafo. (a) *ASYCZBXTD*; (b) nenhum, o grafo não é livre de ciclos, por exemplo, *YBAXSY* é um ciclo; (c) *BTYXACSDZ*

9.40 Ver Fig. 9-38(*a*).

9.41 (a) Ver Fig. 9-38(*b*); (b) Apenas fracamente conexo.

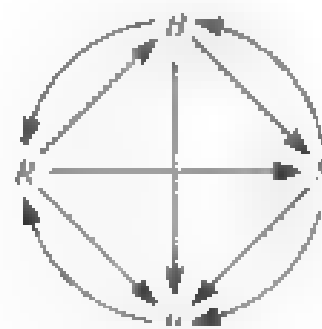
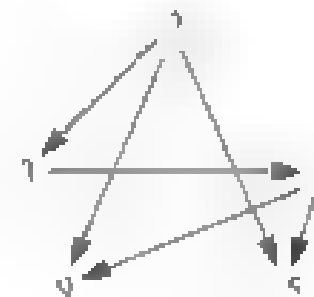
9.42 ***Sugestão*:** Suponha que ($\alpha = v_1, \ldots, v_m$) é um caminho mais longo de *G* e não inclui o vértice *u*. Se (u, v_1) é um arco, então $\beta = (u, \alpha)$ estende α. Logo, (v_1, u) é um arco. Se (u, v_2) é também um arco, então $\beta = (v_1, u, v_2, \ldots, v_m)$ estende α; logo, (v_2, u) é um arco. Analogamente, (v_3, u), . . .,(v_m, u) são arcos. Portanto, $\beta = (\alpha, u)$ estende α. Isso contradiz a maximalidade de α.

(*a*)

(*b*)

Figura 9-38

9.43 (i) $A = [0, 0, 0, 0, 0; 0, 0, 0, 1, 0; 1, 1, 0, 1, 0; 0, 1, 0, 0, 0; 1, 0, 1, 0, 0]$
$P = [1, 1, 1, 1, 1, 0, 1, 0, 1, 0; 1, 1, 1, 1, 1, 0, 1, 0, 1, 0; 1, 1, 1, 1, 1]$
(ii) $A = [0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0; 0, 1, 1, 0, 1, 0; 0, 0, 1, 0, 0, 0; 0, 0, 0, 1, 0, 0]$
$P = [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0; 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0; 1, 1, 1, 1, 1, 1]$

9.44 (i) $W = [7, 5, 0, 0; 0, 0, 0, 2, 0, 3, 0, 0; 4, 0, 1, 0]$, $Q = [AA, AB, ABCD, ABD; BDA, BDCB, BDC, BD; CBDA, CB, CBDC, CBD; DA, DCB, DC, DCBD]$, onde *A*, *B*, *C*, *D* são vértices.

(ii) $W = [0, 0, 1, 0, 5; 0, 0, 0, 1, 0; 0, 0, 0, 4, 3, 2, 0, 0, 0, 0; 0, 2, 0, 4, 0]$; $Q = [ACDA, ACEB, AC, ACD, ACE; BDA, BDACEB, BDAC, BD, BDACE; CDA, CEB, CDAC, CD, CE; DA, DACEB, DAC, DACD, DACEB; EDA, EB, EDAC, ED, EDACE]$, onde *A*, *B*, *C*, *D*, *E* são vértices.

9.45 (a) PILHA: $B, L_B\ E_B, E_L\ C_L\ E_B, F_E\ C_L, D_F\ C_L, C_L, J_C, K_J$, $\varnothing$; Vértices: $B, L_B, E_L, F_E, D_F, C_L, J_C, K_J$

(b) PILHA: E, F_E, D_F, $\varnothing$; Vértices: E, F_E, D_F

(c) PILHA: $K, L_K C_K, E_L C_L, C_K, C_L, D_F C_L, C_L J_C$, $\varnothing$; Vértices: $K, L_K, E_L, F_E, D_F, C_L, J_C$

9.46 FILA. $K, L_K C_K, J_C E_C D_C L_K, J_C E_C D_C, J_C E_C, F_E$; Vértices: $K, C_K, L_K, D_C, E_C, J_C, F_E$; Caminho Mínimo: $F_E \leftarrow E_C \leftarrow C_K \leftarrow$ ou $K \rightarrow C_K \rightarrow E_C \rightarrow F_E$.

Árvores Binárias

10.1 INTRODUÇÃO

A árvore binária é uma estrutura fundamental em matemática e ciência da computação. Parte da terminologia de árvores enraizadas, como aresta, caminho, ramo, folha, profundidade e número de nível, é também empregada para árvores binárias. Contudo, usamos o termo nó, no lugar de vértice, para árvores binárias. Enfatizamos que uma árvore binária não é um caso especial de árvore enraizada; trata-se de objetos matemáticos distintos.

10.2 ÁRVORES BINÁRIAS

Uma *árvore binária T* é definida como um conjunto finito de elementos, chamados de nós, tal que.

(1) T é vazio (chamado de *árvore nula* ou *árvore vazia*), ou

(2) T contém um nó notável R, chamado de *raiz* de T, e os demais nós de T formam um par ordenado de árvores binárias disjuntas T_1 e T_2.

Se T contém uma raiz R, então as duas árvores T_1 e T_2 são chamadas, respectivamente, de subárvores de R à esquerda e à direita. Se T_1 for não vazia, então sua raiz é chamada de *sucessor à esquerda* de R, analogamente, se T_2 é não vazio, então sua raiz é chamada de *sucessor à direita* de R

A definição dada de uma árvore binária T é recursiva, uma vez que T é definida em termos de subárvores binárias T_1 e T_2 Isso significa, em especial, que todo nó N de T contém uma subárvore à esquerda e à direita, e qualquer uma delas pode ser vazia, inclusive ambas. Assim, todo nó N de T admite 0, 1 ou 2 sucessores. Um nó sem sucessores é conhecido como nó *terminal* Portanto, ambas as subárvores de um nó terminal são vazias.

Representação visual de uma árvore binária

Uma árvore binária T é frequentemente apresentada por um diagrama no plano, chamado de *representação visual* de T. Especificamente, o diagrama na Fig. 10-1(a) representa uma árvore binária como se segue.

(i) T consiste em 11 nós, representados pelas letras de A a L, excluindo I.

(ii) A raiz de T é o nó no topo do diagrama.

(iii) Uma linha inclinada para a esquerda e para baixo em um nó N indica um sucessor à esquerda de N, e uma linha inclinada para a direita e para baixo em N corresponde a um sucessor à direita de N

Consequentemente, na Fig. 10-1(a):

(a) B é um sucessor à esquerda, e C é um sucessor à direita da raiz A.

(b) A subárvore à esquerda da raiz A consiste nos nós B, D, E, e F; a subárvore à direita de A é formada pelos nós C, G, H, J, K e L.

(c) Os nós A, B, C e H têm dois sucessores, os nós E e J têm apenas um sucessor, e os nós D, F, G, L e K não admitem sucessores, ou seja, são terminais.

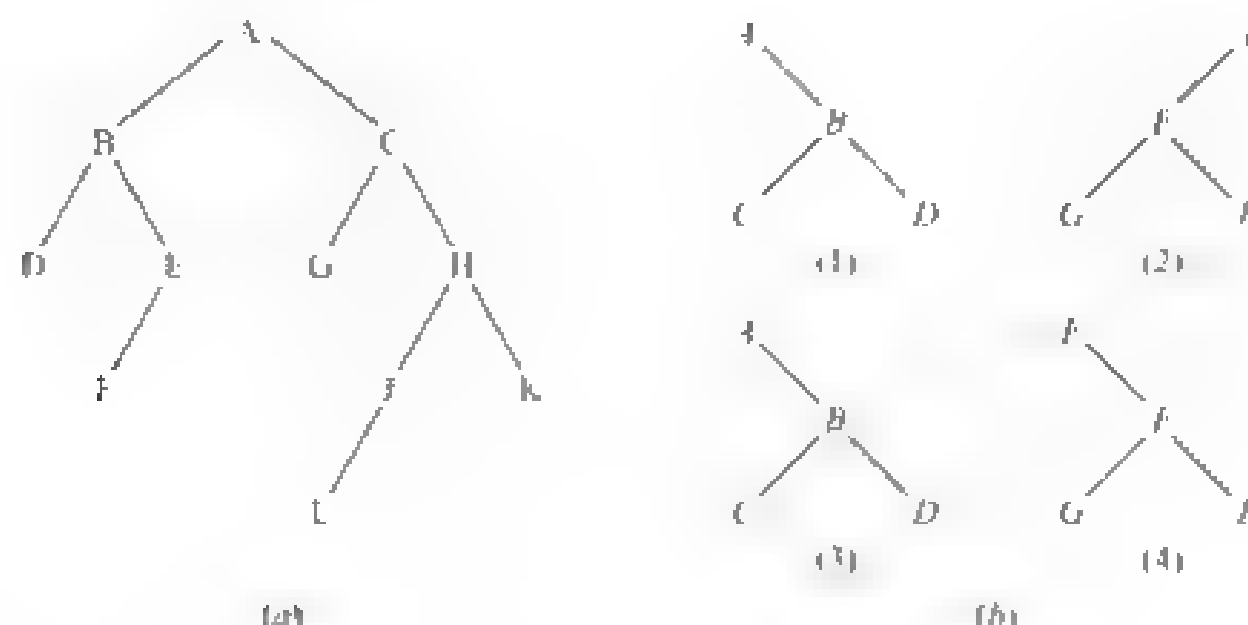



Figura 10-1

Árvores binárias semelhantes

As árvores binárias T e T' são ditas *semelhantes* se têm a mesma estrutura ou, em outras palavras, se compartilham a mesma forma. As árvores são ditas *cópias* se forem semelhantes e se tiverem os mesmos conteúdos nos nós correspondentes.

Exemplo 10.1 Considere as quatro árvores binárias na Fig. 10-1(b). As três árvores (1), (3) e (4) são semelhantes. Em especial, as árvores (1) e (3) são cópias, uma vez que elas têm também os mesmos dados nos nós correspondentes. A árvore (2) não é semelhante nem cópia da árvore (4), pois, em uma árvore binária, distinguimos entre um sucessor à esquerda e um sucessor à direita, mesmo quando existe somente um sucessor.

Terminologia

A terminologia descrevendo relações familiares é frequentemente empregada para descrever relações entre os nós de uma árvore. Especificamente, suponha que N é um nó em T, com sucessor à esquerda S_1 e sucessor à direita S_2. Então, N é chamado de *pai* de S_1 e S_2. Analogamente, S_1 é chamado de *filho à esquerda* de N e S_2, de *filho à direita* de N. Além disso, S_1 e S_2 são ditos *irmãos*. Todo nó N em uma árvore binária T, exceto a raiz, tem um único pai, chamado de *predecessor* de N.

Os termos descendente e ancestral têm seu significado usual. Ou seja, um nó L é dito *descendente* de um nó N (e N é chamado de *ancestral* de L) se existe uma sucessão de filhos de N a L. Em especial, L é chamado de *descendente à esquerda* ou *à direita* de N se L pertence à subárvore à esquerda ou à direita de N.

A terminologia de teoria dos grafos e a de horticultura são também empregadas em uma árvore binária T. Especificamente, uma linha desenhada a partir de um nó N de T até um sucessor é chamada de *aresta*, e uma sequência de arestas consecutivas é conhecida como um *caminho*. Um nó terminal é chamado de *folha* e um caminho terminando em uma folha se chama *ramo*.

Cada nó em uma árvore binária T é assinalado com um *número de nível*, como se segue. A raiz R da árvore T é assinalada ao número de nível 0, e todos os demais nós são designados com um número de nível que é 1 a mais do que o número de nível de seu pai. Além disso, os nós com o mesmo número de nível são ditos pertencerem à mesma *geração*.

A *profundidade* (ou *altura*) de uma árvore T é o número máximo de nós de um ramo de T. Isso corresponde a 1 a mais do que o maior número de nível de T. A árvore T na Fig. 10-1(a) tem profundidade 5.

10.3 ÁRVORES BINÁRIAS COMPLETAS E ESTENDIDAS

Esta seção considera dois casos especiais de árvores binárias.

Árvores binárias completas

Considere qualquer árvore binária T. Cada nó de T pode ter no máximo dois filhos. Consequentemente, é possível mostrar que o nível r de T pode ter no máximo 2^r nós. A árvore T é dita *completa* se todos os seus níveis, exceto, possivelmente o último, têm o número máximo de possíveis nós e se todos os nós no último nível aparecem o mais à esquerda possível. Logo, existe uma única árvore completa T_n com exatamente n nós (onde ignoramos os conteúdos dos nós). A árvore completa T_{26} com 26 nós aparece na Fig. 10-2.

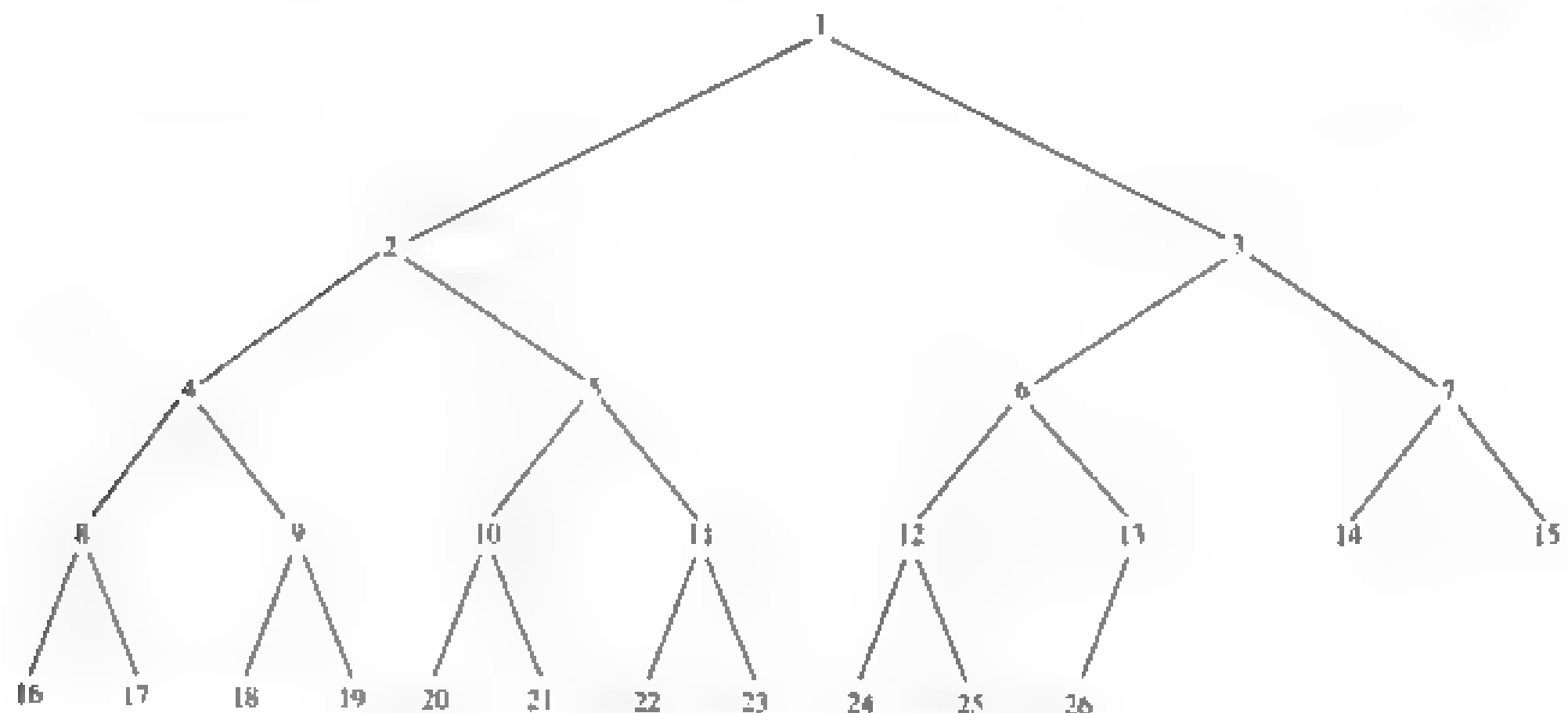



Figura 10-2 Árvore completa T_{26}.

Os nós da árvore binária completa T_{26} da Fig. 10-2 foram intencionalmente rotulados pelos números 1, 2, ..., 26, da esquerda para a direita, geração por geração. Com esses rótulos, pode-se facilmente determinar os filhos e o pai de cada nó K em qualquer árvore completa T_n. De modo específico, os filhos à esquerda e à direita do nó K são, respectivamente, $2*K$ e $2*K + 1$, e o pai de K é o nó $\lfloor K/2 \rfloor$. Por exemplo, os filhos do nó 9 são os nós 18 e 19, e seu pai é o nó $\lfloor 9/2 \rfloor = 4$. A profundidade d_n da árvore completa T_n com n nós é dada por

$$d_n = \lfloor \log_2 n + 1 \rfloor$$

Esse é um número relativamente pequeno. Por exemplo, se a árvore completa T_n tem $n = 1\,000\,000$ nós, então sua profundidade é $d_n = 21$.

Árvores binárias estendidas: 2-árvores

Uma árvore binária T é dita uma 2-*árvore* ou uma *árvore binária estendida* se cada nó N admite 0 ou 2 filhos. Em tal caso, os nós com dois filhos são chamados de *internos*, e aqueles com 0 filhos são os *externos*. Às vezes os nós são distinguidos em diagramas, usando círculos para os internos e quadrados para os externos.

O termo "árvore binária estendida" surge da seguinte operação. Considere qualquer árvore binária T, como a da Fig. 10-3(a). Então T pode ser "convertida" em uma 2 árvore, substituindo cada subárvore vazia por um novo nó, como representado na Fig. 10-3(b). Observe que a nova árvore é, de fato, uma 2-árvore. Além disso, os nós na árvore original T são agora os nós internos na árvore estendida, e os novos nós são os externos. Notamos que se uma 2-árvore tem n nós internos, então ela terá $n + 1$ nós externos.

(a) Árvore binária T. (b) 2-Árvore estendida

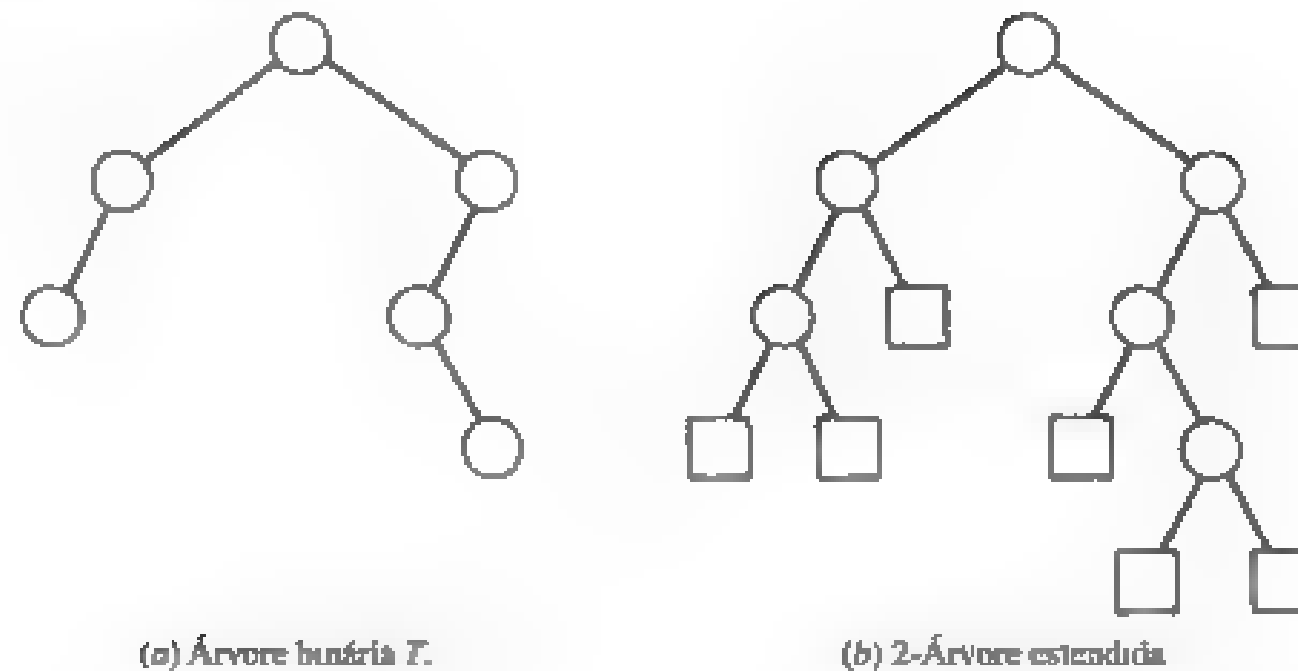



Figura 10-3 Convertendo uma árvore binária *T* em uma 2-árvore.

Expressões algébricas e notação polonesa

Seja *E* uma expressão algébrica qualquer que emprega somente operações binárias, como:

$$E = (a - b)/((c \times d) + e)$$

Então *E* pode ser representada por uma 2-árvore, como na Fig. 10-4(*a*), onde as variáveis em *E* aparecem como os nós externos, e as operações em *E* surgem como nós internos.

O matemático polonês Lukasiewicz observou que, colocando a operação binária antes de seus argumentos, por exemplo,

$$+ab \text{ no lugar de } a + b \text{ e } /cd \text{ no lugar de } c/d$$

não há necessidade de usar quaisquer parênteses. Essa é a chamada de *notação polonesa na forma prefixa*. (Analogamente, podemos colocar o símbolo após seus argumentos, o que corresponde à *notação polonesa na forma pós-fixa*.) Reescrevendo *E* na forma prefixa, obtemos:

$$E = / - a\,b + \times c\,d\,e$$

Observe que esta é precisamente a ordem lexicográfica dos vértices em sua 2-árvore, que pode ser obtida, escaneando a árvore, como na Fig. 10-4(*b*).

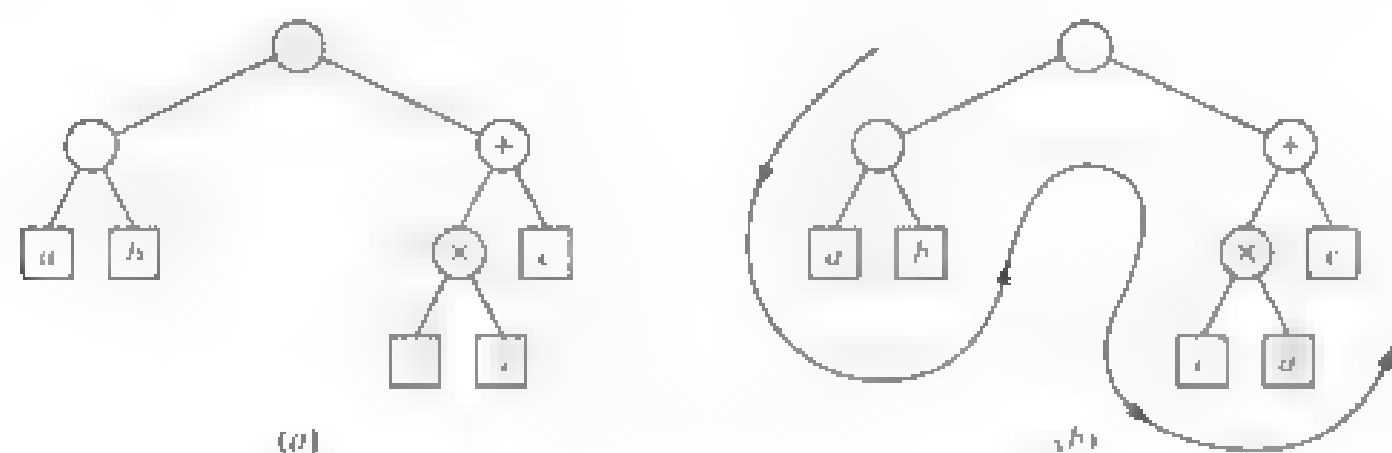



Figura 10-4

10.4 REPRESENTANDO ÁRVORES BINÁRIAS NA MEMÓRIA

Seja *T* uma árvore binária. Esta seção discute duas maneiras para representar *T* na memória. A primeira, que é a usual, é chamada de *representação ligada* de *T* e é análoga ao modo como listas ligadas são representadas na me-

mória. A segunda maneira, que emprega um único array, é conhecida como *representação sequencial* de T. As principais exigências de qualquer representação de T são o acesso direto à raiz R de T e, dado qualquer nó N de T, também devemos ter acesso direto aos filhos de N.

Representação ligada de árvores binárias

Considere uma árvore binária T. A menos que seja dito ou sugerido o contrário, T é mantida na memória por meio de uma representação ligada que emprega três arrays paralelos, INFO, LEFT, RIGHT, e uma variável apontadora ROOT, como se segue. Antes de tudo, cada nó N de T corresponde a uma localização K, de modo que:

(1) INFO[K] contém os dados do nó N

(2) LEFT[K] contém a localização do filho à esquerda do nó N

(3) RIGHT[K] contém a localização do filho à direita do nó N

Além disso, ROOT contém a localização da raiz R de T. Se qualquer subárvore for vazia, então o apontador correspondente contém o valor nulo; se a árvore T em si for vazia, então ROOT contém o valor nulo.

Observação 1: A maioria de nossos exemplos mostram um único item de informação em cada nó N de uma árvore binária T. Na prática, um registro inteiro pode ser armazenado no nó N. Em outras palavras, INFO pode realmente ser um array linear de registros ou uma coleção de arrays paralelos.

Observação 2: Qualquer nome inválido pode ser escolhido para o apontador nulo denotado por NULL. Na prática, 0 ou um número negativo é empregado para NULL.

Exemplo 10.2 Considere a árvore binária T na Fig. 10-1(a). A representação ligada de T aparece na Fig. 10-5, onde escrevemos os arrays na vertical em vez de horizontalmente, por conveniência notacional. Observe que ROOT = 5 aponta para INFO[5] = A, uma vez que A é a raiz de T. Note também que LEFT[5] = 10 aponta para INFO[10] = B, pois B é o filho à esquerda de A, e RIGHT[5] = 2 aponta para INFO[2] = C, uma vez que C é o filho à direita de A, e assim por diante. A escolha de 18 elementos para os arrays é arbitrária.

Figura 10-5

Representação sequencial de árvores binárias

Suponha que T é uma árvore binária completa ou quase completa. Então existe uma maneira eficiente para manter T na memória, conhecida como a *representação sequencial* de T. Tal representação usa somente um array linear TREE em parceria com uma variável apontadora END, como se segue:

(1) A raiz R de T é armazenada em TREE[1].

(2) Se um nó N ocupa TREE[K], então seu filho à esquerda é armazenado em TREE[2*K] e o da direita é armazenado em TREE[2*K + 1].

(3) END contém a localização do último nó de T.

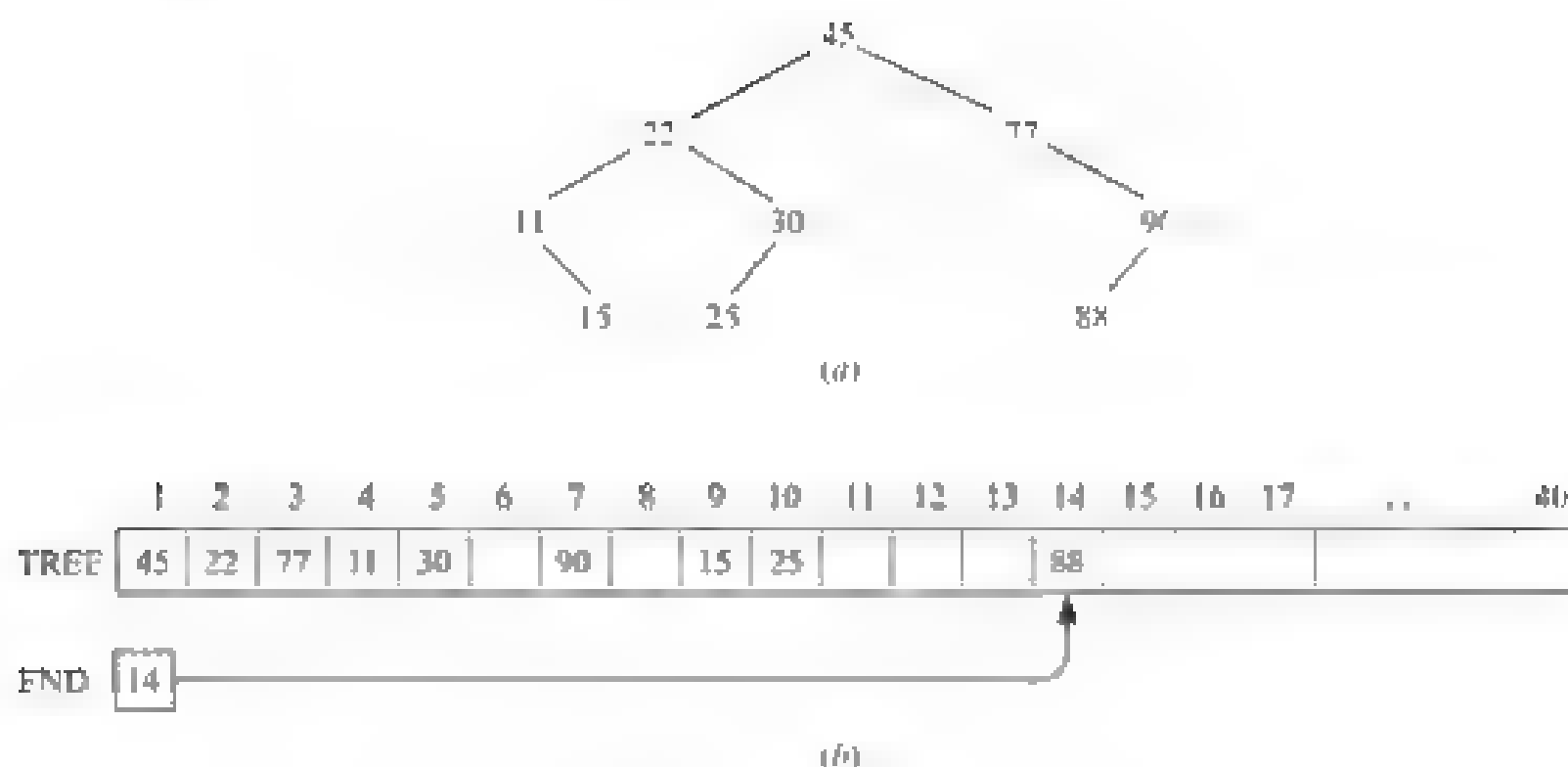



Figura 10-6

Além disso, o nó N em TREE[K] contém uma subárvore vazia à esquerda ou uma subárvore vazia à direita conforme 2^*K ou $2^*K + 1$ exceda END, ou dependendo de TREE[2^*K] ou TREE[$2^*K + 1$] conter o valor NULO.

A representação sequencial da árvore binária T na Fig. 10-6(a) aparece na Fig. 10-6(b). Observe que exigimos 14 localizações no array TREE, apesar de T ter apenas 9 nós. Em termos gerais, a representação sequencial de uma árvore com altura d requer uma sequência com aproximadamente 2^d elementos. Consequentemente, essa representação sequencial é em geral ineficiente, a menos que, como recém-colocado, a árvore binária T seja completa ou quase completa. Por exemplo, a árvore T na Fig. 10-1(a) tem 11 nós e profundidade 5, o que significa que ela exige uma sequência com aproximadamente $2^5 = 32$ elementos.

10.5 PERCORRENDO ÁRVORES BINÁRIAS

Existem três maneiras usuais de percorrer uma árvore T com raiz R. Esses três algoritmos, chamados de *pré-ordem*, *inordem* e *pós-ordem* são como se seguem:

Pré-ordem: (1) Processe a raiz R.
(2) Percorra a subárvore à esquerda de R em pré-ordem.
(3) Percorra a subárvore à direita de R em pré-ordem.

Inordem: (1) Percorra a subárvore à esquerda de R em inordem.
(2) Processe a raiz R.
(3) Percorra a subárvore à direita de R em inordem.

Pós-ordem: (1) Percorra a subárvore à esquerda de R em pós-ordem.
(2) Percorra a subárvore à direita de R em pós-ordem.
(3) Processe a raiz R.

Note que cada algoritmo contém os mesmos três passos e que a subárvore à esquerda de R é sempre percorrida antes da subárvore à direita. A diferença entre os algoritmos é o momento em que a raiz é processada. Especificamente, no algoritmo "pré", a raiz R é processada antes que as subárvores sejam percorridas, no algoritmo "in", a raiz R é processada entre os percursos das subárvores, no algoritmo "pós", a raiz R é processada depois que as subárvores foram percorridas.

Os três algoritmos são, às vezes, chamados respectivamente de percursos nó-esquerda-direita (NLR, na sigla em inglês), esquerda-nó-direita (LNR) e esquerda-direita-nó (LRN).

Exemplo 10.3 Considere a árvore binária T na Fig. 10-7(a). Observe que A é a raiz de T, a subárvore L_T à esquerda de T consiste nos nós B, D e E e que a subárvore R_T à direita de T é formada pelos nós C e F.

(a) O percurso pré-ordem de T processa A, percorre L_T e percorre R_T. Porém, o percurso pré-ordem de L_T processa a raiz B e, em seguida, D e E; e o percurso pré-ordem de R_T processa a raiz C e então F. Assim, *ABDECF* é o percurso pré-ordem de T.

(b) O percurso inordem de T percorre L_T, processa A e percorre R_T. No entanto, o percurso inordem de L_T processa D, B e, em seguida, E; e o percurso inordem de R_T processa C e depois F. Desse modo, *DBEACF* é o percurso inordem de T.

(c) O percurso pós-ordem de T percorre L_T e processa A. Contudo, o percurso pós-ordem de L_T processa D, E e depois B, e o percurso pós-ordem de *RT* processa F e, em seguida, C. Consequentemente, *DEBFCA* é o percurso pós-ordem de T.

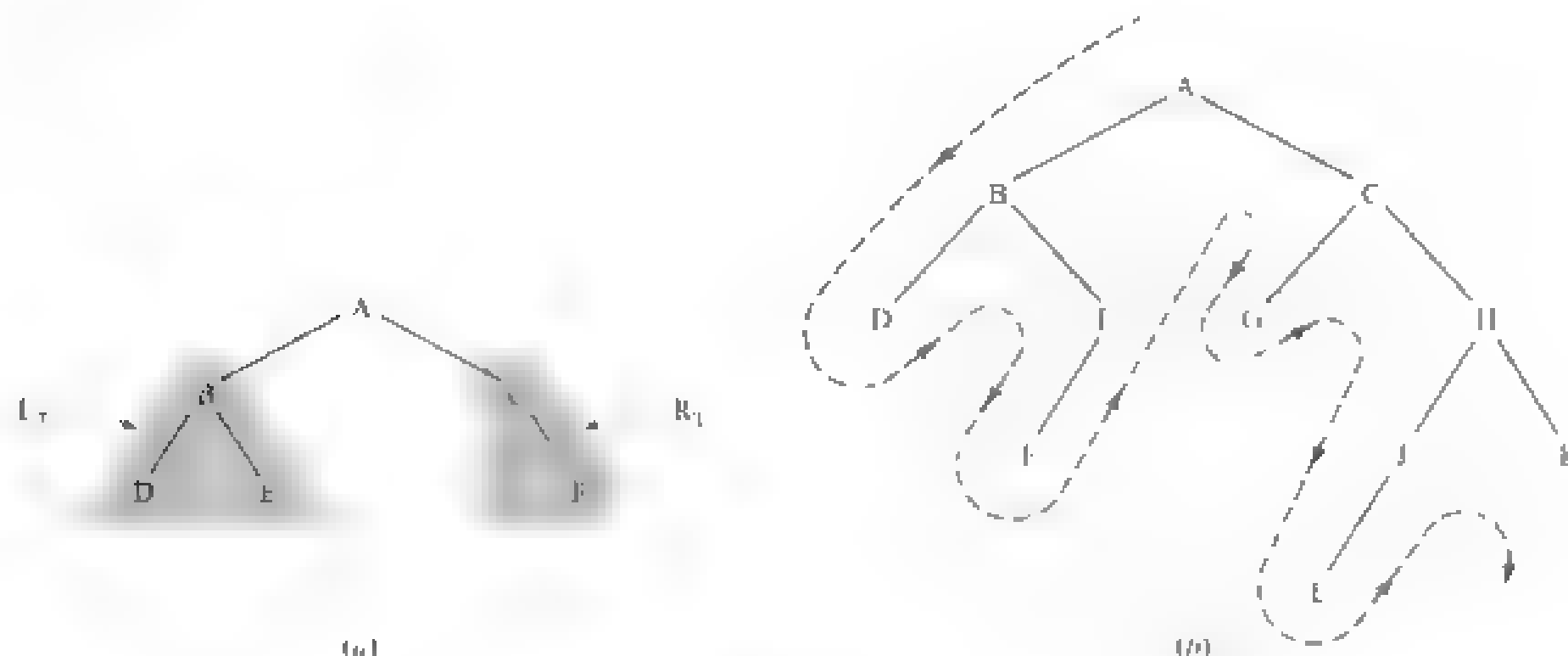



Figura 10-7

Exemplo 10.4 Seja T a árvore binária na Fig. 10-7(b). O percurso pré-ordem é como se segue:

(Pré-ordem) *A B D E F C G H J L K*

Essa ordem é a mesma obtida, escaneando a árvore a partir da esquerda, como indicado pelo caminho na Fig. 10-7(b). Ou seja, segue-se para baixo pelo ramo da extrema esquerda até encontrar um nó terminal e, em seguida, retorna-se para o próximo ramo, e assim por diante. No percurso pré-ordem, o nó terminal mais à direita, K, é o último escaneado. Observe que a subárvore à esquerda da raiz A é percorrida antes da subárvore da direita, e ambas são percorridas depois de A. O mesmo vale para qualquer outro nó que admite subárvores, que é a propriedade subjacente de um percurso pré-ordem.

O leitor pode verificar por inspeção que as outras duas maneiras de percorrer a árvore T na Fig. 10-7(b) são como se segue:

(Inordem) *D B F E A G C L J H K*
(Pós-ordem) *D F E B G L J K H C A*

Observação: Note que os nós terminais D, F, G, L e K da árvore binária na Fig. 10-7(b) são percorridos na mesma ordem, da esquerda para a direita, em todos os percursos. Enfatizamos que isso é verdadeiro para qualquer árvore binária T.

10.6 ÁRVORES BINÁRIAS DE BUSCA

Esta seção discute uma das mais importantes estruturas de dados em ciência da computação, uma árvore binária de busca. Tal estrutura permite buscar e encontrar um elemento com um tempo médio de processamento de

$f(n) = 0(\log_2 n)$, onde n é o número de itens dos dados. Também facilmente permite inserir e deletar elementos. Essa estrutura contrasta com as seguintes:

(a) *Array linear ordenado:* Aqui pode-se buscar e encontrar um elemento com tempo de processamento de $f(n) = 0(\log_2 n)$. No entanto, inserir e deletar elementos é caro, uma vez que, na média, envolve o deslocamento de $0(n)$ elementos.

(b) *Lista ligada:* Aqui podemos facilmente inserir e deletar elementos. Porém, é caro para buscar e encontrar um elemento, pois se deve usar uma busca linear com tempo de processamento de $f(n) = 0(n)$.

Apesar de cada nó em uma árvore binária de busca poder conter um registro inteiro de dados, a definição da árvore depende de um dado campo cujos valores são distintos e podem ser ordenados.

Definição: Suponha que T é uma árvore binária. Então T é chamada de *árvore binária de busca* se cada nó N de T tem a seguinte propriedade:

> O valor de N é maior do que todo valor na subárvore à esquerda de N e é menor do que todo valor na subárvore à direita de N.

Não é difícil perceber que a propriedade acima garante que o percurso inordem de T nos leva a uma lista ordenada dos elementos de T.

Observação: A definição dada de árvore binária de busca assume que todos os valores de nós são distintos. Há uma definição análoga de árvore binária de busca T que admite duplicatas, ou seja, na qual cada nó N tem as propriedades a seguir:

(a) $N > M$ para cada nó M em uma subárvore à esquerda de N.

(b) $N < M$ para cada nó M em uma subárvore à direita de N.

Quando essa definição é empregada, as operações discutidas abaixo devem ser modificadas de acordo.

Exemplo 10.5 A árvore binária T na Fig. 10-8(a) é uma árvore binária de busca. Isto é, todo nó N em T excede cada número em subárvore à esquerda e é menor do que cada número em sua subárvore à direita. Suponha que 23 fosse substituído por 35. Então T ainda seria uma árvore binária de busca. Por outro lado, suponha que 23 fosse substituído por 40. Então T não seria uma árvore binária de busca, pois 40 estaria na subárvore de 38, porém, $40 > 38$.

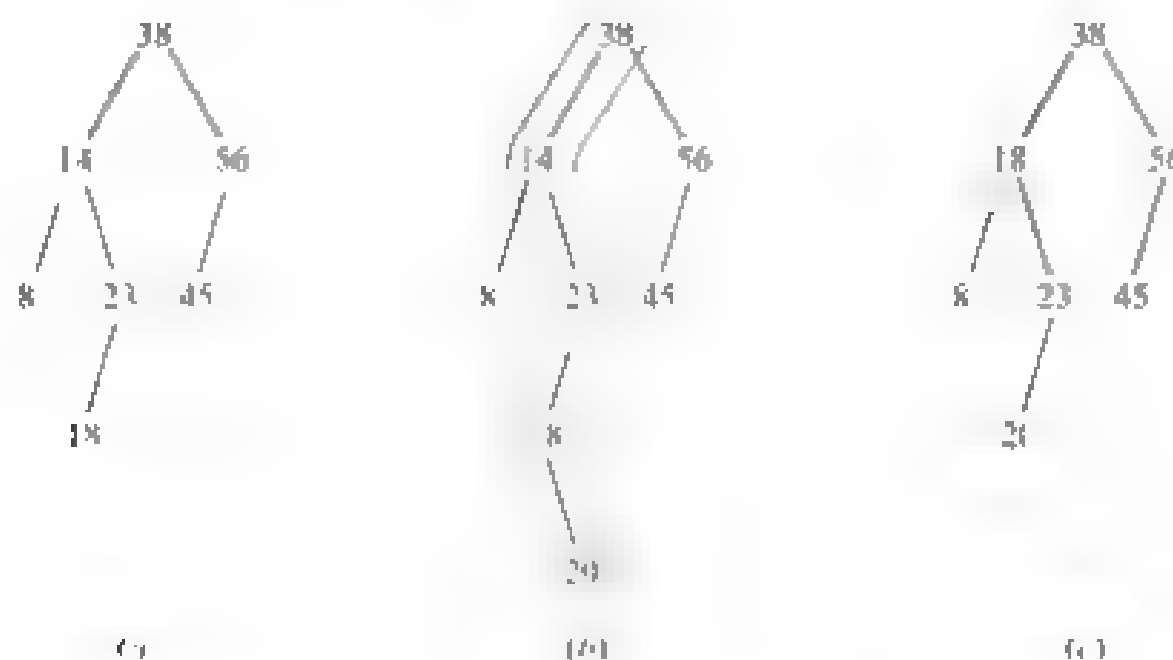



Figura 10-8

Buscando e inserindo em uma árvore binária de busca

Um algoritmo de busca e inserção em uma árvore binária de busca T aparece na Fig. 10-9.

Algoritmo 10.1: Uma árvore binária de busca T e um ITEM de informação são dados. O algoritmo encontra a localização de ITEM em T, ou insere ITEM como novo nó na árvore.

Passo 1. Compare ITEM com a raiz N da árvore.

(*a*) Se ITEM $<N$, proceda para o filho à esquerda de N.

(*b*) Se ITEM $>N$, proceda para o filho à direita de N

Passo 2. Repita o Passo 1 até ocorrer o seguinte:

(*a*) Encontramos um nó N tal que ITEM $=N$. Neste caso, a busca é bem-sucedida.

(*b*) Encontramos uma subárvore vazia, o que indica que a busca é malsucedida. Insira ITEM no lugar da subárvore vazia.

Passo 3. Saída.

Figura 10-9

Exemplo 10.6 Considere a árvore binária de busca T na Fig. 10-8(*a*). Suponha que ITEM $=20$ seja dado, e queremos encontrar ou inserir ITEM em T. Simulando o Algoritmo 10-1, obtemos os passos a seguir:

(1) Compare ITEM $=20$ com raiz $R=38$. Como $20<38$, procedemos para o filho à esquerda de 38, que é 14

(2) Compare ITEM $=20$ com 14. Como $20>14$, procedemos para o filho à direita de 14, que é 23.

(3) Compare ITEM $=20$ com 23. Como $20<23$, proceda para o filho à esquerda de 23, que é 18

(4) Compare ITEM $=20$ com 18. Como $20>18$ e 18 não tem filho à direita, insira 20 como o filho à direita de 18

A Fig. 10-8(*b*) mostra a nova árvore com ITEM $=20$ inserida. O caminho para baixo, na árvore, durante o algoritmo foi salientado.

Deletando em uma árvore binária de busca

Um algoritmo que deleta um dado ITEM de uma árvore binária de busca T aparece na Fig. 10-10. Ele emprega o Algoritmo 10.1 na Fig. 10-9 para encontrar a localização do ITEM em T.

Observação: Note que o caso (iii) no Passo 2(c) é mais complicado do que os dois primeiros casos. O sucessor inordem $S(N)$ de N é encontrado como se segue. A partir do nó N, mova diretamente para o filho à direita de N e então, sucessivamente, vá para a esquerda até encontrar um nó M sem filho à esquerda. O nó M é o sucessor inordem $S(N)$ de N

Exemplo 10.7 Considere a árvore binária na Fig. 10-8(*b*). Suponha que queremos deletar ITEM $=14$ de T. Primeiro encontramos o nó N tal que $N=14$. Note que $N=14$ tem dois filhos. Movendo para a direita e então para esquerda, encontramos o sucessor inordem $S(N)=18$ de N. Deletamos $S(N)=18$, substituindo-o por seu único filho 20 e, então, substituímos $N=14$ por $S(N)=18$. Isso nos leva à árvore na Fig. 10-8(*c*)

Complexidade dos algoritmos de árvore binária de busca

Seja T a árvore binária com n nós e profundidade d, e seja $f(n)$ o tempo de processamento de qualquer um dos algoritmos acima. O Algoritmo 10.1 nos diz para proceder da raiz R, seguindo a árvore T até encontrar ITEM em T ou inserir ITEM como nó terminal. O Algoritmo 10.2 nos diz para proceder a partir da raiz R, através da árvore T, para encontrar ITEM e então continuar para baixo, ao longo da árvore T, para encontrar o sucessor inordem de ITEM. Em qualquer caso, o número de movimentos não pode exceder a profundidade d da árvore. Assim, o tempo de processamento $f(n)$ de qualquer um dos algoritmos depende da profundidade d da árvore T.

Algoritmo 10.2: Uma árvore binária de busca T e um ITEM de informação são dados. $P(N)$ denota o pai de um nó N, e $S(N)$ corresponde ao sucessor inordem de N. O algoritmo deleta ITEM de T

Passo 1. Use Algoritmo 10.1 para encontrar a localização do nó que contém ITEM e rastreie a localização do nó pai $P(N)$ (Se ITEM não estiver em T, então pare (STOP) e vá para a saída.)

Passo 2. Determine o número de filhos de N. Há três casos

(*a*) **N não tem filhos.** N é deletado de T, simplesmente substituindo a localização de N no nó pai $P(N)$ pelo apontador NULL.

(*b*) **N tem exatamente um filho M** N é deletado de T, substituindo a localização de N no nó pai $P(N)$ pela localização de M (Isso troca N por M)

(*c*) **N tem dois filhos.**

(i) Encontre o sucessor inordem $S(N)$ de N. (Então $S(N)$ não tem filho à esquerda)

(ii) Delete $S(N)$ de T, usando (*a*) ou (*b*).

(iii) Substitua N por $S(N)$ em T.

Passo 3. Saída.

Figura 10-10

Agora suponha que T tem a propriedade de que, para qualquer nó N de T, as profundidades das subárvores de N diferem no máximo em 1. Então a árvore T é dita equilibrada e $d \approx \log_2 n$. Portanto, o tempo de processamento $f(n)$ de qualquer algoritmo em uma árvore equilibrada é muito rápido; especificamente, $f(n) = 0(\log_2 n)$. Por outro lado, à medida que itens são adicionados em uma árvore binária de busca T, não há garantia de que T permaneça equilibrada. Poderia até mesmo acontecer de $d \approx n$. Neste caso, $f(n)$ seria relativamente lento, especificamente, $f(n) = 0(n)$. Felizmente, existem técnicas para reequilibrar uma árvore binária de busca T à medida que elementos são adicionados a T Tais técnicas, porém, estão além do escopo deste texto.

10.7 FILAS DE PRIORIDADE, HEAPS

Seja S uma fila de prioridade. Ou seja, S é um conjunto cujos elementos podem ser periodicamente inseridos e deletados, mas no qual o maior elemento corrente (aquele com mais alta prioridade) é sempre deletado. Pode-se manter S na memória como se segue:

(a) **Array linear:** Aqui se pode facilmente inserir um elemento, apenas adicionando-o ao final do array Contudo, é caro buscar e encontrar o maior elemento, uma vez que se deve usar uma busca linear com tempo de processamento $f(n) = 0(n)$.

(b) **Array linear ordenado:** Aqui o maior elemento é o primeiro ou o último e, assim, é facilmente deletado No entanto, inserir e deletar elementos é caro, pois, na média, envolve $0(n)$ elementos.

Esta seção introduz uma estrutura discreta que pode implementar de modo eficiente uma fila de prioridade S

Heaps

Suponha que H é uma árvore binária completa com n elementos. Assumimos que H é mantida na memória, usando sua representação sequencial e não uma representação ligada. (Ver Seção 10.4.)

Definição 10.1: Suponha que H é uma árvore binária completa. Então H é chamada de *heap*, ou *heap máximo*, se cada nó tem a seguinte propriedade.

O valor de N é maior ou igual ao valor de cada um dos filhos de N

Consequentemente, em um heap o valor de N excede o valor de cada um de seus descendentes. A raiz de H, em especial, é um valor maior de H.

Um *heap mínimo* é definido de forma análoga: O valor de N é menor ou igual ao valor de cada um de seus filhos.

Exemplo 10.8 Considere a árvore binária completa H na Fig. 10-11(a). Observe que H é um heap. Isso significa, principalmente, que o maior elemento de H aparece no "topo" do heap. A Fig. 10-11(b) mostra a representação sequencial de H pelo array TREE e pela variável END. Consequentemente:

(a) TREE[1] é a raiz R de H.

(b) TREE[$2K$] e TREE[$2K + 1$] são os filhos à esquerda e à direita de TREE[K].

(c) A variável END = 20 aponta para o último elemento de H.

(d) O pai de qualquer nó TREE(J) diferente da raiz é o nó TREE[$J \div 2$] (onde $J \div 2$ é a divisão entre inteiros).

Observe que os nós de H sobre o mesmo nível aparecem um após o outro no array TREE. A escolha de 30 localizações para TREE é arbitrária.

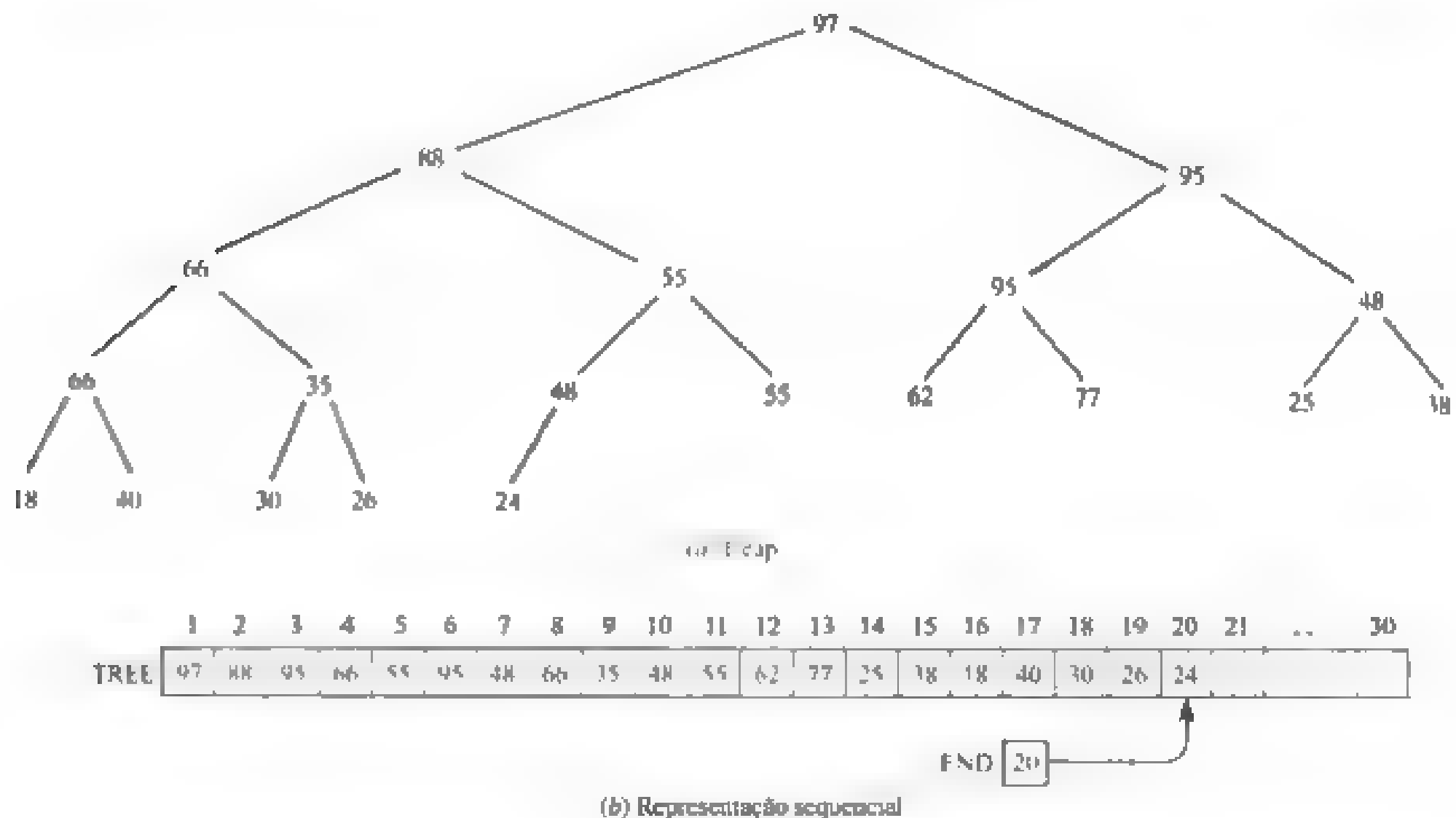



Figura 10-11

Inserindo em um heap

A Fig. 10-12 fornece um algoritmo que insere um ITEM de dados em um heap H

Observação: Deve-se verificar que o Algoritmo 10.3 sempre conduz a um heap como árvore final. Isso não é difícil de perceber, e deixamos tal verificação para o leitor.

Exemplo 10.9 Considere o heap H na Fig. 10-11. Suponha que queremos inserir ITEM = 70 em H. Simulando o Algoritmo 10.3, primeiro juntamos ITEM ao último elemento da árvore completa, isto é, como o filho à direita de 48.

Algoritmo 10.3: Um heap H e um novo ITEM são dados. O algoritmo insere ITEM em H.

Passo 1. Junte ITEM no final de H, de modo que H ainda seja uma árvore completa, mas não necessariamente um heap.

Passo 2. (Refaça o heap) Deixe ITEM subir para seu "lugar apropriado" em H, de modo que H seja um heap. Isto é:

(*a*) Compare ITEM com seu pai P(ITEM). Se ITEM > P(ITEM), então permute ITEM e P(ITEM).

(*b*) Repita (*a*) até ITEM ≤ P(ITEM).

Passo 3. Saída.

Figura 10-12

Em outras palavras, fazemos TREE[21] = 70 e END = 21. Então refaça o heap, ou seja, deixamos ITEM subir para seu lugar adequado como se segue:

(a) Compare ITEM = 70 com seu pai 48. Como 70 > 48, permutamos 70 e 48.

(b) Compare ITEM = 70 com seu novo pai 55. Como 70 > 55, permutamos 70 e 55

(c) Compare ITEM = 70 com seu pai 88 Como 70 < 88, ITEM = 70 subiu para seu lugar apropriado no heap H.

A Fig. 10-13 mostra a árvore final H com ITEM = 70 inserido. O caminho pela árvore por ITEM foi circundado.

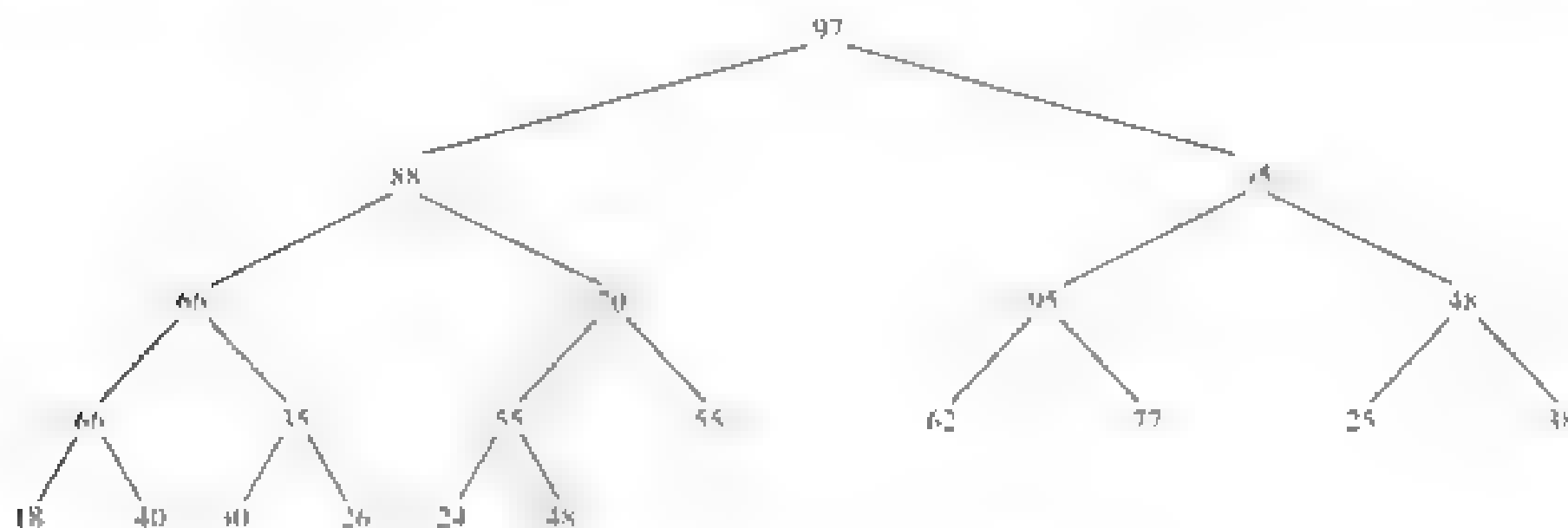



Figura 10-13 ITEM = 70 é inserido.

Deletando a raiz de um heap

A Fig. 10-14 fornece um algoritmo que deleta a raiz R de um heap H.

Observação: Como no caso de inserção em um heap, devemos verificar que o Algoritmo 10.4 sempre conduz a um heap como árvore final. Novamente, deixamos essa verificação para o leitor Notamos também que o Passo 3 pode não terminar até que o nó L alcance a base da árvore, ou seja, até que L não tenha filhos

Exemplo 10.10 Considere o heap H na Fig. 10-15(*a*), onde $R = 95$ é a raiz e $L = 22$ é o último nó de H Suponha que queremos deletar $R = 95$ do heap H Simulando o Algoritmo 10.4, primeiro "deletamos" $R = 95$, assinalando ITEM = 95, e então substituímos $R = 95$ por $L = 22$. Isso nos leva à árvore completa da Fig. 10-15(*b*), que não é um heap. (Note que ambas as subárvores de 22 ainda são heaps.) Em seguida, nós refazemos o heap, ou seja, fazemos $L = 22$ cair até seu lugar adequado como se segue:

Algoritmo 10.4: O algoritmo deleta a raiz R de um dado heap H.

Passo 1. Assinale a raiz R a alguma variável ITEM.

Passo 2. Substitua a raiz deletada R pelo último nó de L de H, de modo que H ainda seja uma árvore binária completa, mas não necessariamente um heap. [Ou seja, faça TREE[1] = TREE[END] e então faça END := END−1.]

Passo 3. (Refaça o heap) Faça L cair para seu "lugar apropriado" em H, de modo que H seja um heap. Isto é:

(*a*) Encontre o maior filho LARGE(L) de L. Se $L <$ LARGE(L), então permute L e LARGE(L)

(*b*) Repita (*a*) até $L >$ LARGE(L).

Passo 4. Saída.

Figura 10-14

(a) Os filhos de $L = 22$ são 85 e 70. O maior é 85. Como $22 < 85$, permutamos 22 e 85. Isso nos leva à árvore na Fig. 10-15(*c*).

(b) Os filhos de $L = 22$ são agora 33 e 55. O maior é 55. Como $22 < 55$, permutamos 22 e 55. Isso nos leva à árvore na Fig. 10-15(*d*).

(c) Os filhos de $L = 22$ são agora 15 e 11. O maior é 15. Como $22 > 15$, o nó $L = 22$ caiu para seu lugar apropriado no heap.

Assim, a Fig. 10-15(*d*) é o heap H pedido sem sua raiz original $R = 95$. Observe que destacamos os caminhos à medida que $L = 22$ seguiu seu percurso para baixo na árvore.

Complexidade dos algoritmos de heap

Seja H um heap com n nós. Como H é uma árvore completa, $d \approx \log_2 n$, onde d é a profundidade de H. O Algoritmo 10.3 nos diz para deixar o novo ITEM proceder árvore acima, de nível a nível, até encontrar seu lugar apro-

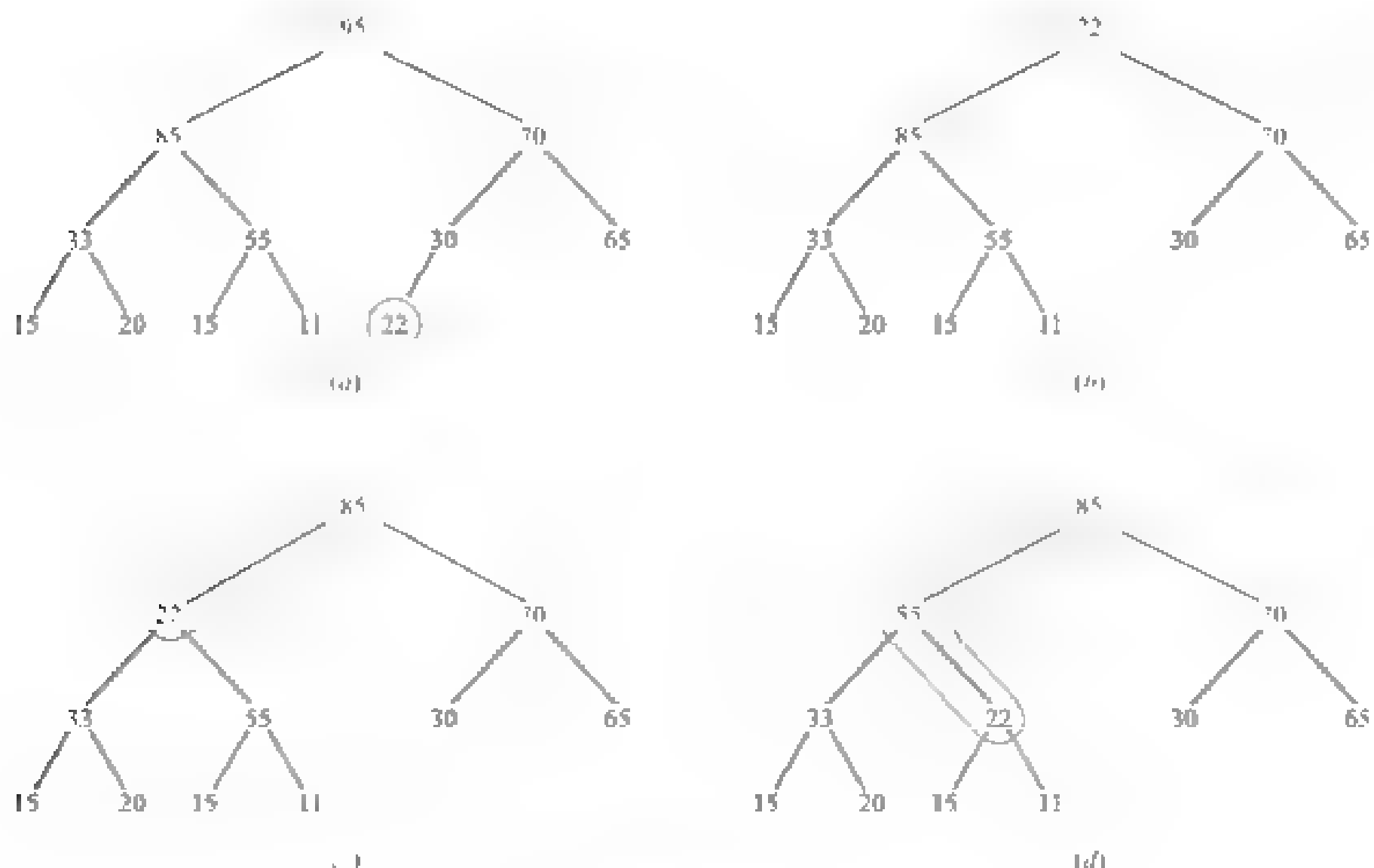



Figura 10-15

priado em H. O Algoritmo 10.4 nos diz para deixar o último nó original L proceder árvore abaixo, nível por nível, até encontrar seu lugar adequado em H. Em qualquer caso, o número de movimentos não pode exceder a profundidade d de H. Assim, o tempo de processamento $f(n)$ de qualquer um dos algoritmos é muito rápido, especificamente, $f(n) = O(\log_2 n)$. Consequentemente, o heap é uma maneira muito mais eficiente para implementar uma fila de prioridade S do que o array linear ou o array linear ordenado mencionados no começo da seção.

10.8 COMPRIMENTO DE CAMINHO, ALGORITMO DE HUFFMAN

Seja T uma árvore binária estendida ou 2-árvore (Seção 10.3). Lembre que se T tem n nós externos, então T tem $n - 1$ nós internos. A Fig. 10-3(b) mostra uma 2-árvore com sete nós externos e, consequentemente, $7 - 1 = 6$ nós internos.

Comprimento de caminho ponderado

Suponha que T é uma 2-árvore com n nós externos e que cada um deles é assinalado a um peso (não negativo). O comprimento do caminho ponderado (ou simplesmente comprimento do caminho) P da árvore T é definido como a soma

$$P = W_1L_1 + W_2L_2 + \cdots + W_nL_n$$

onde W_i é o peso em um nó externo N_i, e L_i é o comprimento do caminho da raiz R ao nó L_i. (O comprimento do caminho P existe mesmo para 2-árvores não ponderadas, onde simplesmente se assume o peso 1 em cada nó externo.)

Exemplo 10.11 A Fig. 10-16 mostra três 2-árvores, T_1, T_2 e T_3, cada uma tendo nós externos com os mesmos pesos 2, 3, 5 e 11. Os comprimentos dos caminhos ponderados das três árvores são como se segue:

$$P_1 = 2(2) + 3(2) + 5(2) + 11(2) = 42$$
$$P_2 = 2(1) + 3(3) + 5(3) + 11(2) = 48$$
$$P_3 = 2(3) + 3(3) + 5(2) + 11(1) = 36$$

As quantidades P_1 e P_3 indicam que a árvore completa não precisa dar um caminho mínimo, e que as quantidades P_2 e P_3 indicam que as árvores semelhantes não precisam resultar no mesmo comprimento de caminho.

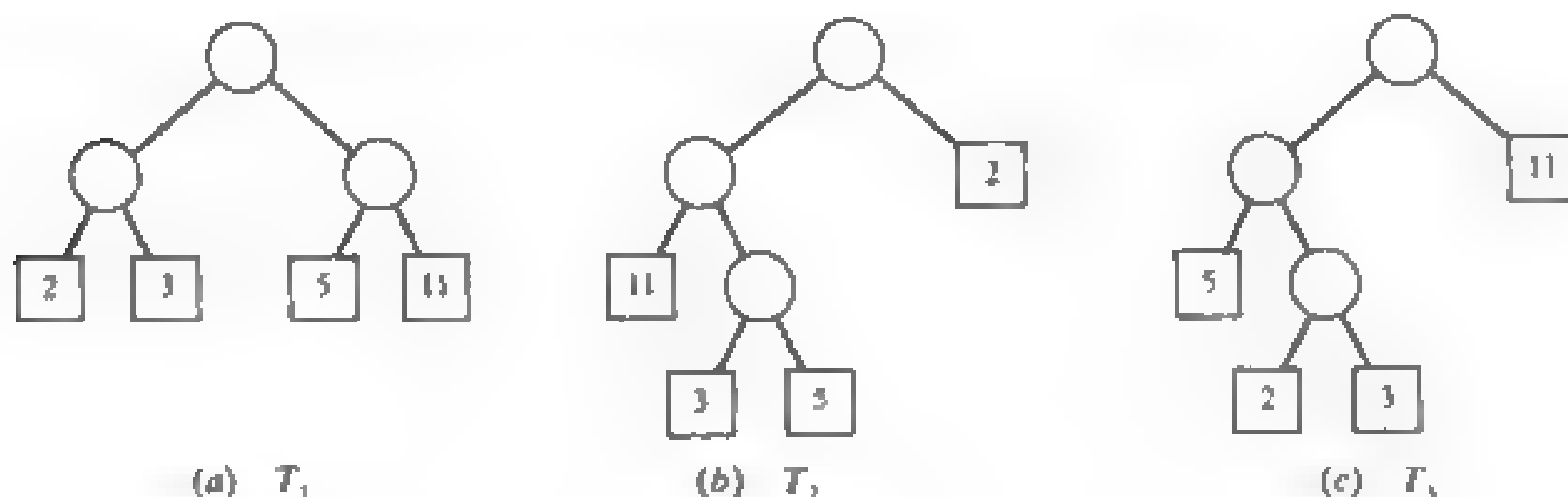



Figura 10-16

Algoritmo de Huffman

O problema geral que queremos resolver é o seguinte. Suponha que uma lista de n pesos seja dada:

$$W_1, W_2, \ldots, W_n$$

Entre todas as 2-árvores com n nós externos e com os n pesos dados, encontre uma árvore T com um comprimento de caminho ponderado mínimo. (Tal árvore é raramente única.) Huffman criou um algoritmo para encontrar tal árvore T.

O algoritmo de Huffman, que aparece na Fig. 10-17, é recursivamente definido em termos do número n de pesos. Na prática, usamos uma forma iterativa equivalente do algoritmo de Huffman que constrói a árvore T desejada de baixo para cima, em vez de cima para baixo.

Algoritmo 10.5 (Huffman): O algoritmo encontra recursivamente uma 2-árvore ponderada T com n pesos dados $w_1, w_2, \ldots, w_n$ que tem um comprimento de caminho ponderado mínimo.

Passo 1. Suponha que $n = 1$. Seja T a árvore com um nó N com peso w_1, então vá para a Saída.

Passo 2. Suponha que $n > 1$.

(*a*) Encontre dois pesos mínimos, digamos w_i e w_j, entre os n pesos dados.

(*b*) Substitua w_i e w_j na lista por $w_i + w_j$, de modo que a lista tenha $n - 1$ pesos.

(*c*) Encontre uma árvore T' que fornece um comprimento de caminho ponderado mínimo para os $n - 1$ pesos.

(*d*) Na árvore T', substitua o nó externo

(*e*) Saída.

Figura 10-17

Exemplo 10.12 Sejam A, B, C, D, E, F, G, H oito itens de dados com os seguintes pesos designados.

Item de dados:	A	B	C	D	E	F	G	H
Peso:	22	5	11	19	2	11	25	5

Construa uma 2-árvore T com um comprimento de caminho ponderado mínimo P, usando os dados acima como nós externos.

Aplique o algoritmo de Huffman. Ou seja, combine repetidamente as duas subárvores com pesos mínimos em uma única subárvore, como mostrado na Fig. 10-18(*a*). Para fins de clareza, os pesos originais são sublinhados, e um número circulado indica a raiz de uma nova subárvore. A árvore T é esboçada a partir do Passo 8 para trás, levando à Fig. 10-18(*b*). (Quando quebramos um nó em duas partes, esboçamos o menor nó à esquerda.) O comprimento do caminho P é o que se segue:

$$P = 22(2) + 11(3) + 11(3) + 25(2) + 5(4) + 2(5) + 5(5) + 19(3) = 280$$

Implementação computacional do algoritmo de Huffman

Considere novamente os dados do Exemplo 10.12. Suponha que queremos implementar o algoritmo, usando o computador. Uma vez que alguns dos nós de nossa árvore binária são ponderados, ela pode ser mantida por quatro arrays paralelos: INFO, WT, LEFT e RIGHT (informação, peso, esquerda, direita, respectivamente). As oito primeiras colunas na Fig. 10-19 mostram como os dados podem ser inicialmente armazenados no computador.

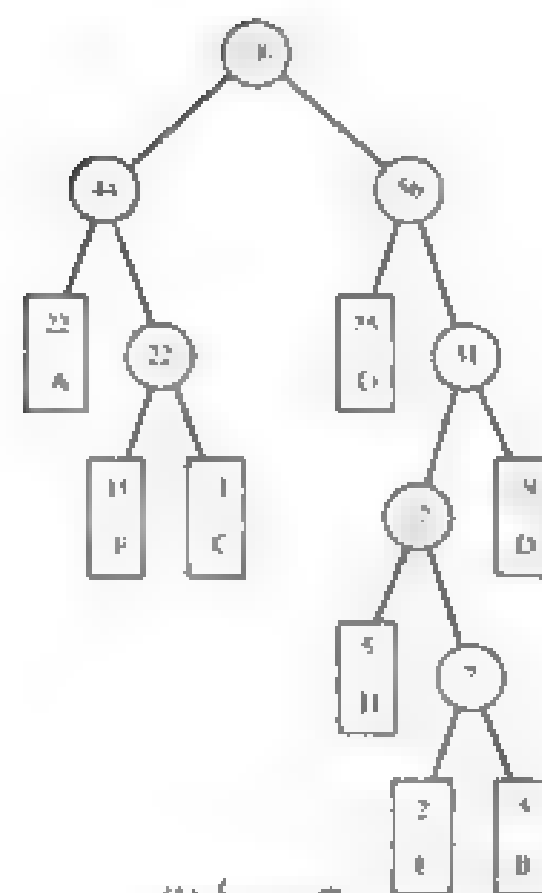
Cada passo no algoritmo de Huffman designa valores para WT, LEFT e RIGHT nas colunas de 9 a 15, o que corresponde, respectivamente, aos passos (2) a (8) na Fig. 10-18. Especificamente, cada passo encontra os dois pesos mínimos correntes e suas localizações, e então entra a soma em WT e suas localizações em LEFT e RIGHT. Por exemplo, os pesos mínimos correntes após designar valores à coluna 11, o que corresponde ao passo (4), são

(a) Algoritmo de Huffman (b) Árvore T

Figura 10-18

12 e 19, que aparecem em WT[10] e WT[4]. Logo, designamos WT[12] = 12 + 19 = 31 e LEFT[12] = 10 bem como RIGHT[12] = 4. O último passo nos diz que ROOT = 15, ou usamos o fato de que ROOT = $2n - 1$, onde $n = 8$ é o número de nós externos. Assim, a Fig. 10-19 fornece a árvore T desejada.

Figura 10-19

Observação: Durante a execução do algoritmo de Huffman, precisamos rastrear os pesos correntes e encontrar dois dos pesos mínimos. Isso pode ser conseguido de modo eficiente, mantendo um heap mínimo auxiliar, onde cada nó contém um peso e sua localização na árvore. Usamos um heap mínimo em vez de um heap máximo, pois queremos o nó com o menor peso no topo do heap.

Aplicação em codificação

Suponha que uma coleção de n dados $A_1, A_2, \ldots, A_n$ sejam codificados por meio de strings de bits.† Além disso, suponha que os itens de dados não ocorram com a mesma probabilidade. Então, o espaço de memória e o tempo podem ser conservados, usando strings com comprimento variável, onde itens que ocorrem com frequência são designados como strings mais curtos e os que ocorrem com menos frequência são assinalados como strings mais longos. Por exemplo, códigos de telefone de países usam esse princípio. O código para os Estados Unidos é simplesmente 1, para a França é 33 e para a Finlândia é 358. Esta seção discute uma codificação que emprega comprimento variável baseado na *árvore de Huffman T* para itens de dados ponderados, isto é, uma 2-árvore T com comprimento de caminho mínimo P.

Código de Huffman: Seja T a árvore de Huffman para os n itens de dados ponderados $A_1, A_2, \ldots, A_n$. Cada aresta de T é assinalada 0 ou 1, dependendo se a aresta aponta para um filho à esquerda ou à direita. A codificação de Huffman assinala a cada nó externo A_i a sequência de bits da raiz R da árvore ao nó A_i. O código de Huffman citado

† N. de T.: Sequências finitas de bits.

tem a propriedade "prefixo", ou seja, o código de qualquer item não é um substring inicial do código de qualquer outro item. Isso significa que não pode haver ambiguidade alguma na decodificação de qualquer mensagem usando um código de Huffman.

Exemplo 10.13 Considere novamente os oito itens de dados A, B, C, D, E, F, G, H do Exemplo 10.12. Suponha que os pesos representam as probabilidades percentuais de que os itens ocorrem. Assinalando, como na página anterior, rótulos de bits às arestas na árvore de Huffman da Fig. 10-18(b), ou seja, 0 ou 1, dependendo se a aresta aponta para um filho à esquerda ou à direita, obtemos a seguinte codificação para os dados:

$$A: 00, \quad B: 11011, \quad C: 011, \quad D: 111,$$
$$E: 11010, \quad F: 010, \quad G: 10, \quad H: 1100.$$

Por exemplo, para chegar a E, a partir da raiz, o caminho consiste em uma aresta à direita, aresta à direita, aresta à esquerda, aresta à direita e aresta à esquerda, levando ao código 11010 para E.

10.9 ÁRVORES GERAIS (ORDENADAS E ENRAIZADAS) REVISITADAS

Seja T uma árvore ordenada enraizada (Seção 9.4), que é também conhecida como *árvore geral*. T pode ser formalmente definida como um conjunto não vazio de elementos, chamados de nós, tal que:

(1) T contém um elemento distinto R, chamado de *raiz* de T.

(2) Os outros elementos de T formam uma coleção ordenada de zero ou mais árvores disjuntas $T_1, T_2, \ldots, T_n$.

As árvores $T_1, T_2, \ldots, T_n$ são *subárvores* da raiz R, e as raízes de $T_1, T_2, \ldots, T_n$ são chamadas de *sucessores* de R.

A terminologia de relações familiares, teoria dos grafos e horticultura é empregada em árvores gerais da mesma maneira que se faz em árvores binárias. Principalmente, se N é um nó com sucessores $S_1, S_2, \ldots, S_n$, então N é chamado de *pai* do S_i, S_i é chamado de filho de N e os S_i são irmãos um do outro.

Exemplo 10.14 A Fig. 10-20(a) é uma representação visual de uma árvore geral T com 13 nós,

$$A, B, C, D, E, F, G, H, J, K, L, M, N$$

A não ser que seja dito o contrário, a raiz de uma árvore T é o nó no topo do diagrama, e os filhos de um nó são ordenados da esquerda para a direita. Portanto, A é a raiz de T, e A tem três filhos; o primeiro, B, o segundo, C e o terceiro, D. Observe que:

(a) C tem três filhos.

(b) Tanto B quanto K têm dois filhos.

(c) Tanto D quanto H têm apenas um filho.

(d) E, F, G, L, J, M e N não têm filhos.

O último grupo de nós, aqueles sem filhos, são chamados de *nós terminais*.

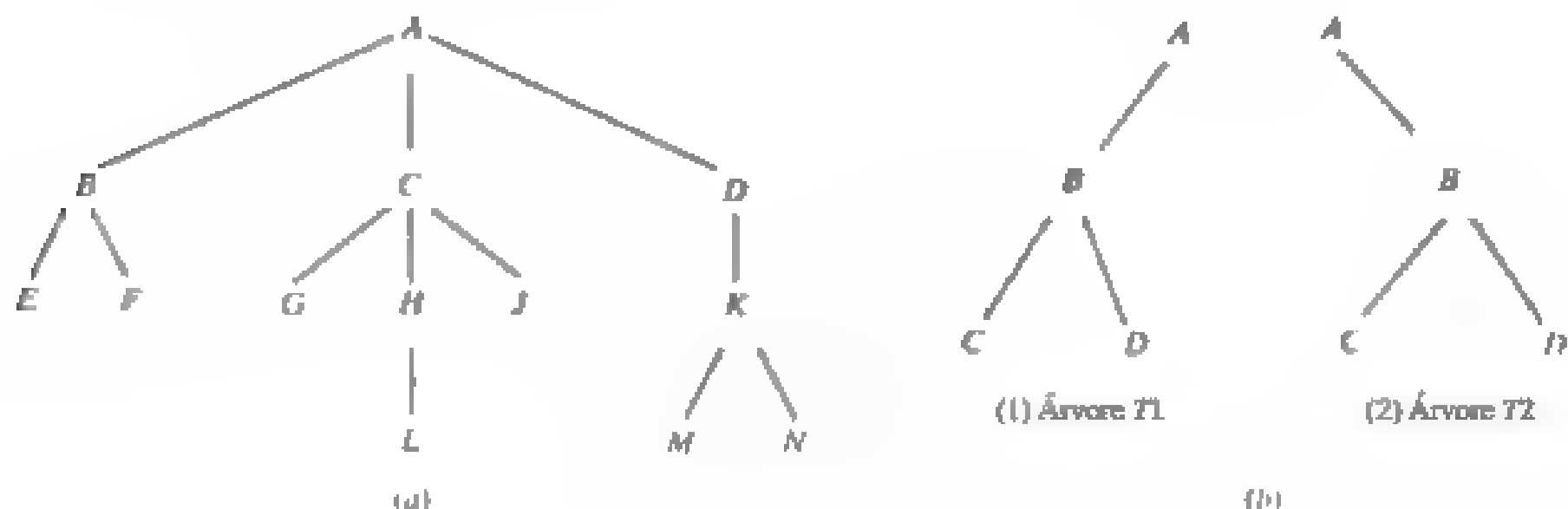



Figura 10-20

Observação: Uma árvore binária T não é um caso especial de árvore geral. Elas são dois objetos diferentes. As duas diferenças básicas são as que se seguem.

(1) Uma árvore binária T' pode ser vazia, mas uma árvore geral T é não vazia.

(2) Suponha que um nó N tem um único filho. Então esse filho é distinguido como à esquerda ou à direita em uma árvore binária T', mas tal diferenciação não existe em uma árvore geral T.

A segunda diferença é ilustrada pelas árvores T_1 e T_2 na Fig. 10-20(*b*). Especificamente, enquanto árvores binárias, T_1 e T_2 são distintas, uma vez que B é o filho à esquerda de A na árvore T_1, mas B é o filho à direita de A na árvore T_2. Por outro lado, não há diferenciação entre as árvores T_1 e T_2 enquanto árvores gerais.

Floresta

Uma *floresta F* é definida como uma coleção ordenada de zero ou mais árvores gerais distintas. Claramente, se deletamos a raiz R de uma árvore geral T, então obtemos a floresta F consistindo nas subárvores de R (que podem ser vazias). Reciprocamente, se F é uma floresta, então podemos acrescentar um nó R a F, para formar uma árvore geral T na qual R é a raiz de T e as subárvores de R consistem nas árvores originais em F.

Árvores gerais e binárias

Suponha que T é uma árvore geral. Então podemos assinalar uma única árvore binária T' a T como se segue. Em primeiro lugar, os nós da árvore binária T' são os mesmos da árvore geral T, e a raiz de T' é a raiz de T. Seja N um nó arbitrário da árvore binária T'. Então o filho à esquerda de N em T' é o primeiro filho do nó N na árvore geral T, e o filho à direita de N em T' é o próximo irmão de N na árvore geral T. Tal correspondência é ilustrada no Problema 10.16.

Problemas Resolvidos

Árvores binárias

10.1 Suponha que T é a árvore binária armazenada na memória, como na Fig. 10-21. Desenhe o diagrama de T.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
INFO	20	30	40	50	60	70	80	90			35	45	55	95
LEFT	0	1	0	0	2	0	0	7			0	3	11	0
RIGHT	0	13	0	0	6	8	0	14			12	4	0	0

RAIZ 5

Figura 10-21

A árvore T é esboçada a partir de sua raiz R para baixo como se segue:

(*a*) A raiz R é obtida a partir do valor do apontador ROOT. Note que ROOT = 5. Logo, INFO[5] = 60 é a raiz R de T.

(*b*) O filho à esquerda de R é conseguido a partir do campo apontador esquerdo de R. Note que LEFT[5] = 2. Logo, INFO[2] = 30 é o filho à esquerda de R.

(*c*) O filho à direita de R é conseguido a partir do campo apontador direito de R. Note que RIGHT[5] = 6. Logo, INFO[6] = 70 é o filho à direita de R.

Podemos agora esboçar a parte superior da árvore e, então, repetindo o processo com cada novo nó, finalmente obtemos a árvore T inteira na Fig. 10-22(*a*).

10.2 Considere a árvore binária T na Fig. 10-22(*b*).

(*a*) Encontre a profundidade d de T.

(*b*) Percorra T, usando o algoritmo de pré-ordem.

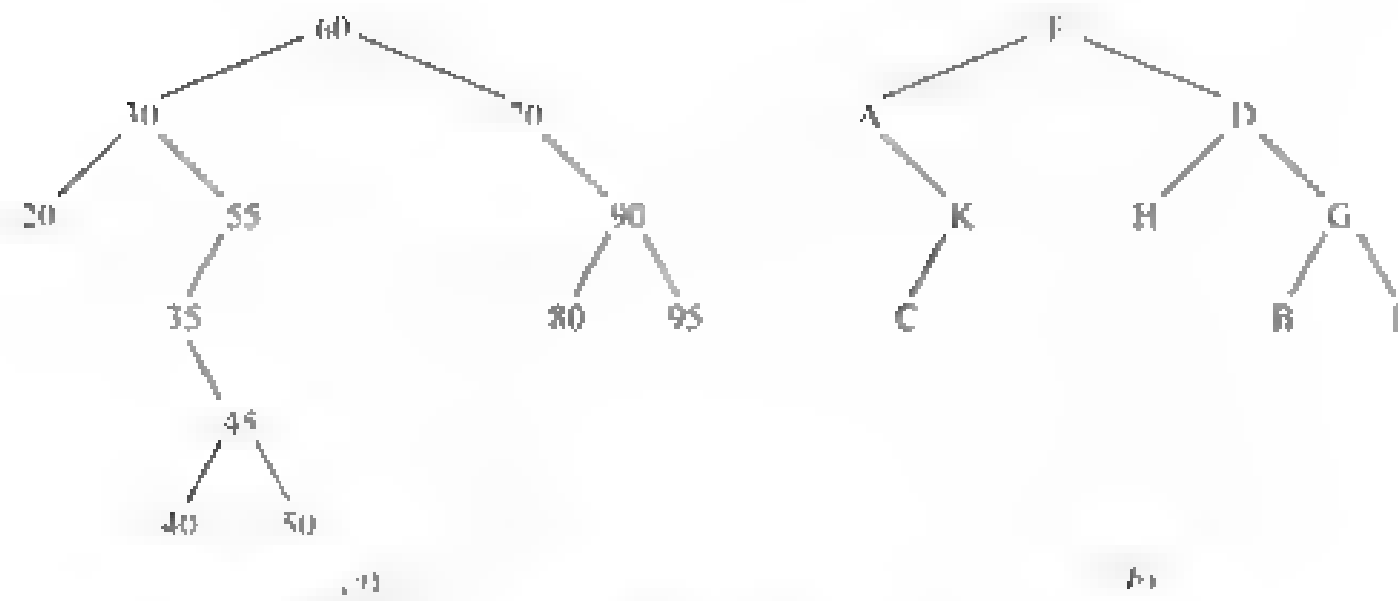



Figura 10-22

(c) Percorra T, usando o algoritmo inordem.

(d) Percorra T, usando o algoritmo pós-ordem.

(e) Encontre os nós terminais de T e a ordem em que eles são percorridos em (b), (c) e (d).

(a) A profundidade d é o número de nós no mais longo ramo de T; logo, $d = 4$.

(b) O percurso pré-ordem de T é um algoritmo recursivo NLR, ou seja, primeiro, ele processa um nó N, em seguida, sua subárvore L à esquerda e, finalmente, sua subárvore à direita R. Denotando $[A_1, \ldots, A_k]$ como uma subárvore com nós $A_1, \ldots, A_k$, a árvore T é percorrida como se segue:

$$F-[A, K, C][D, H, G, B, E] \text{ ou } F-A-[K, C]-D-[H][G, B, E]$$

ou, finalmente,

$$F-A-K-C-D-H-G-B-E$$

(c) O percurso inordem de T é um algoritmo recursivo LNR, isto é, primeiro processa uma subárvore L à esquerda, em seguida, seu nó e, finalmente, sua subárvore à direita R. Assim, T é percorrida como se segue:

$$[A, K, C]-F-[D, H, G, B, E] \text{ ou } A-[K, C]-F-[H]-D-[G, B, E]$$

ou, finalmente,

$$A-K-C-F-H-D-B-G-E$$

(d) O percurso pós-ordem de T é um algoritmo recursivo LRN, ou seja, primeiro, processa uma subárvore à esquerda L, em seguida, sua subárvore à direita R e, finalmente, seu nó N. Logo, T é percorrida como se segue:

$$[A, K, C][D, H, G, B, E]-F \text{ ou } [K, C]-A-[H][G, B, E]-D-F$$

ou, finalmente,

$$C-K-A-H-B-E-G-D-F$$

(e) Os nós terminais são aqueles sem filhos. Eles são percorridos na mesma ordem em todos os três algoritmos de percurso: C, H, B, E.

10.3 Seja T a árvore binária na Fig. 10-22(b). Encontre a representação sequencial de T na memória.

A representação sequencial de T emprega apenas um array TREE e uma variável apontadora END.

(a) A raiz R de T é armazenada em TREE[1]; logo, R = TREE[1] = F.

(b) Se o nó N ocupa TREE[K], então seus filhos à esquerda e à direita são armazenados em TREE[2*K] e TREE[2*K + 1], respectivamente. Logo, TREE[2] = A e TREE[3] = D, uma vez que A e D são os filhos à esquerda e à direita de F, e assim por diante. A Fig. 10-23 contém a representação sequencial de T. Observe que TREE[10] = C, pois C é o filho à esquerda de K, que é armazenado em TREE[5]. Além disso, TREE[14] = B e TREE[15] = E, pois B e E são os filhos à esquerda e à direita de G, que é armazenado em TREE[7].

(*c*) END aponta para a localização do último nó de T; logo, END = 15.

Finalmente, obtemos a representação sequencial de T na Fig. 10-23.

Figura 10-23

10.4 Considere as árvores T_1, T_2 e T_3 na Fig. 10-24. Identifique aquelas que representam a mesma

(*a*) árvore enraizada; (*b*) árvore ordenada enraizada, (*c*) árvore binária.

(*a*) Todas representam a mesma árvore enraizada, ou seja, A é a raiz com filhos (sucessores imediatos) B e C, e C tem um único filho D.

(*b*) Aqui T_1 e T_2 são a mesma árvore ordenada enraizada, mas T_3 é diferente. Especificamente, B é o primeiro filho de A em T_1 e T_2, porém o segundo filho de A em T_3.

(*c*) Todas representam diferentes árvores binárias. Especificamente, T_1 e T_2 são distintas, pois diferenciamos entre sucessores à esquerda e à direita, mesmo quando há um único sucessor (o que não é verdade para árvores ordenadas enraizadas.) Ou seja, D é um sucessor à esquerda de C em T_1, mas um sucessor à direita de C em T_2.

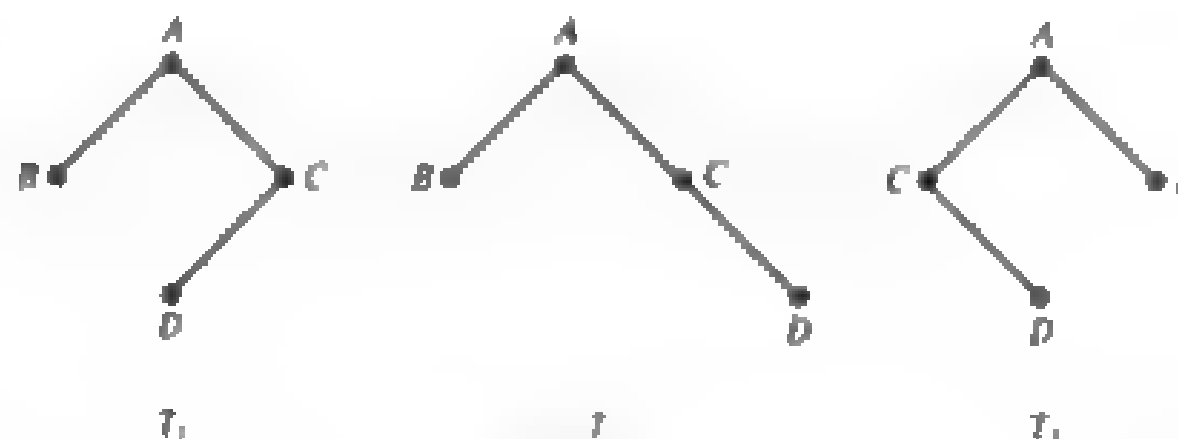



Figura 10-24

10.5 Uma árvore binária T tem nove nós. Esboce uma representação visual de T se o percurso pré-ordem e inordem de T levam às seguintes sequências de nós:

Pré-ordem:	G	B	Q	A	C	P	D	E	R
Inordem:	Q	B	C	A	G	P	E	D	R

A árvore T é esboçada a partir de sua raiz R para baixo como se segue.

(*a*) A raiz de T é obtida, escolhendo o primeiro nó em sua pré-ordem. Assim, G é a raiz de T.

(*b*) O filho à esquerda do nó G é conseguido como se segue. Primeiro, empregamos a inordem de T para encontrar os nós na subárvore à esquerda T_1 de G. Assim, T_1 consiste nos nós Q, B, C, A, que estão à esquerda de G na inordem de T. Em seguida, o filho à esquerda de G é obtido, escolhendo o primeiro nó (raiz) na pré-ordem de T_1, que aparece na pré-ordem de T. Portanto, B é o filho à esquerda de G.

(*c*) Analogamente, a subárvore à direita T_2 de G consiste nos nós P, E, D, R; e P é a raiz de T_2, isto é, P é o filho à direita de G.

Repetindo o processo acima com cada novo nó, finalmente conseguimos a árvore T exigida na Fig. 10-25(*a*).

10.6 Considere a expressão algébrica $E = (2x + y)(5a - b)^3$

(*a*) Desenhe a 2 árvore correspondente. (*b*) Use T para escrever E na forma prefixa polonesa.

(*a*) Use uma flecha (↑) para exponenciação, um asterisco (*) para multiplicação e uma barra (/) para divisão, para obter a árvore da Fig. 10-25(*b*).

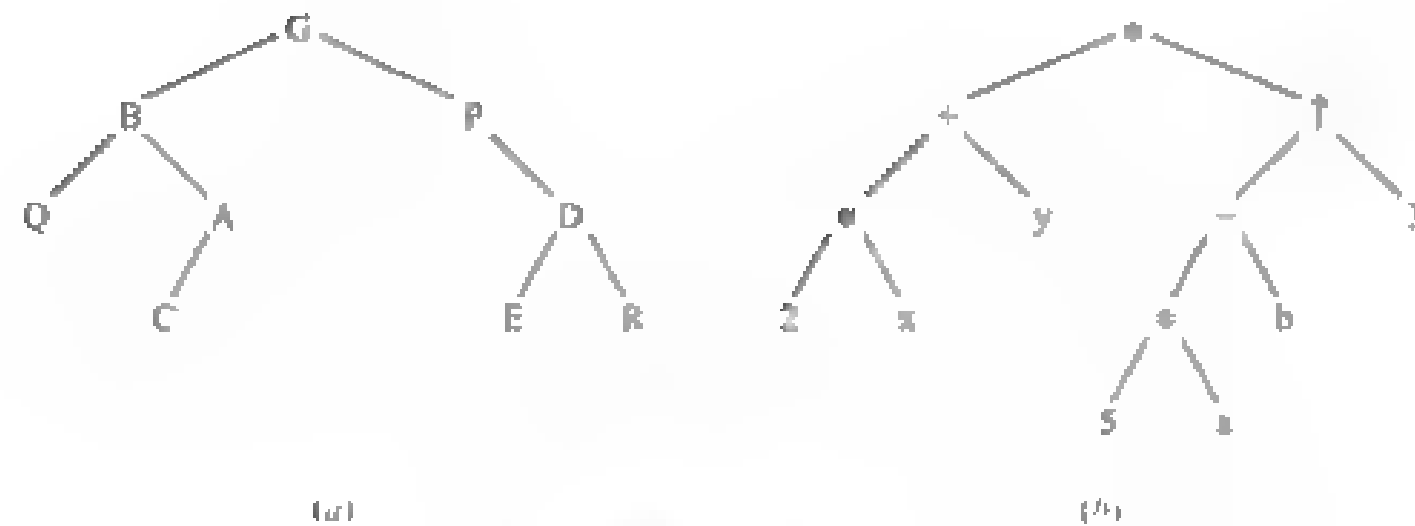



Figura 10-25

(*b*) Escaneie a árvore a partir da esquerda, como na Fig. 10-4(*b*), para obter

$$* + * 2\,x\,y \uparrow - * 5\,a\,b\,3$$

10.7 Esboce todas as possíveis e não semelhantes: (*a*) árvores binárias *T* com três nós, (*b*) 2-árvores *T* ′ com quatro nós externos.

(*a*) Existem cinco árvores como essas, as quais são representadas na Fig. 10-26(*a*).

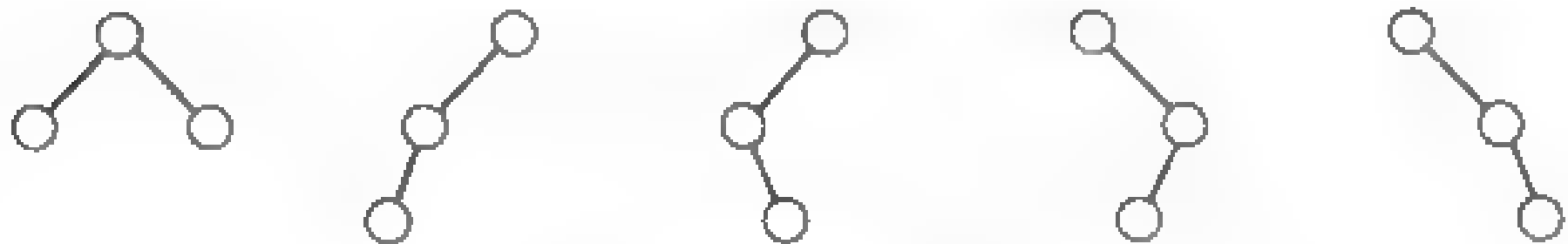
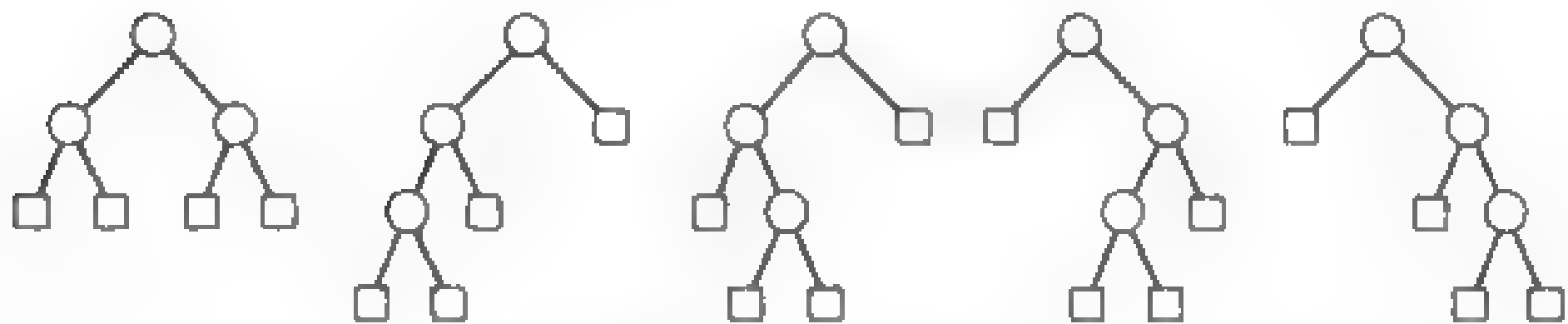
(*b*) Cada 2-árvore *T* ′ com quatro nós externos é determinada por uma árvore binária *T* com três nós, ou seja, por uma árvore *T* no item (*a*). Logo, há cinco 2-árvores *T* ′ como essas, as quais são representadas na Fig. 10-26(*b*).

(*a*) Árvores binárias com 3 nós

(*b*) Árvores binárias estendidas com 4 nós

Figura 10-26

Árvores binárias de busca, heaps

10.8 Considere a árvore binária *T* na Fig. 10-22(*a*).

(*a*) Por que *T* é uma árvore binária de busca?

(*b*) Suponha que ITEM = 33 é adicionado à árvore. Encontre a nova árvore *T*.

(*a*) *T* é uma árvore binária de busca, porque cada nó *N* é maior do que os valores em sua subárvore à esquerda e menor do que os valores em sua subárvore à direita.

(*b*) Compare ITEM = 33 com a raiz 60. Como 33 < 60, mova para o filho à esquerda, 30. Como 33 > 30, mova para o filho à direita, 55. Uma vez que 33 < 55, mova para o filho à esquerda, 35. Agora, 33 < 35, mas 35 não admite filho à esquerda.

Logo, adicione ITEM = 35 como um filho à esquerda do nó 35, para termos a árvore da Fig. 10-27(*a*). As arestas sombreadas indicam o caminho para baixo, através da árvore, durante a inserção.

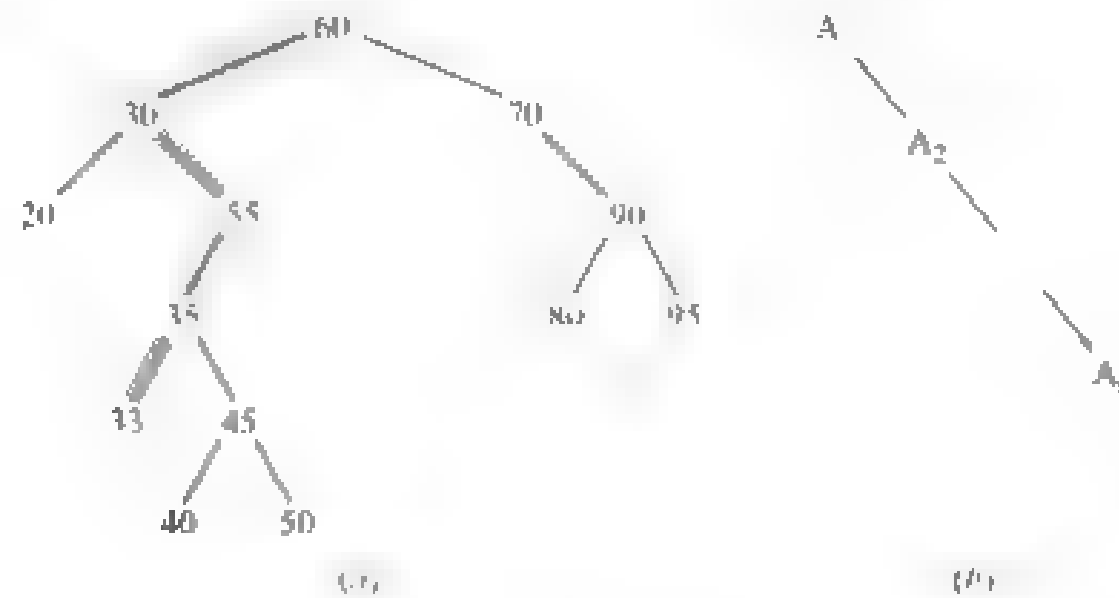



Figura 10-27

10.9 Suponha que *n* itens de dados $A_1, A_2, \ldots, A_N$ já foram ordenados, isto é, $A_1 < A_2 < \cdots < A_N$.

(*a*) Se os itens são inseridos em ordem em uma árvore binária vazia *T*, descreva a árvore final *T*.

(*b*) Qual a profundidade *d* da árvore final *T*?

(*c*) Compare *d* com a profundidade média d^* de uma árvore binária com *n* nós, para (i) $n = 50$; (ii) $n = 100$; (iii) $n = 500$.

(*a*) A árvore *T* consiste em um ramo que se estende para a direita, como retratado na Fig. 10-27(*b*).

(*b*) O ramo de *T* tem *n* nós; logo, $d = n$.

(*c*) Sabe-se que $d^* = c \log_2 n$, onde $c \approx 1{,}4$. Logo, (i) $d(50) = 50$, $d^*(50) \approx 9$; (ii) $d(100) = 100$, $d^*(100) \approx 10$; (iii) $d(500) = 500$, $d^*(500) \approx 12$.

10.10 Suponha que a seguinte lista de letras é inserida em uma árvore binária vazia.

$$J, R, D, G, W, E, M, H, P, A, F, Q$$

(*a*) Encontre a árvore final *T*. (*b*) Encontre o percurso inordem de *T*.

(*a*) Insira os nós, um após o outro, para obter a árvore *T* da Fig. 10-28(*a*).

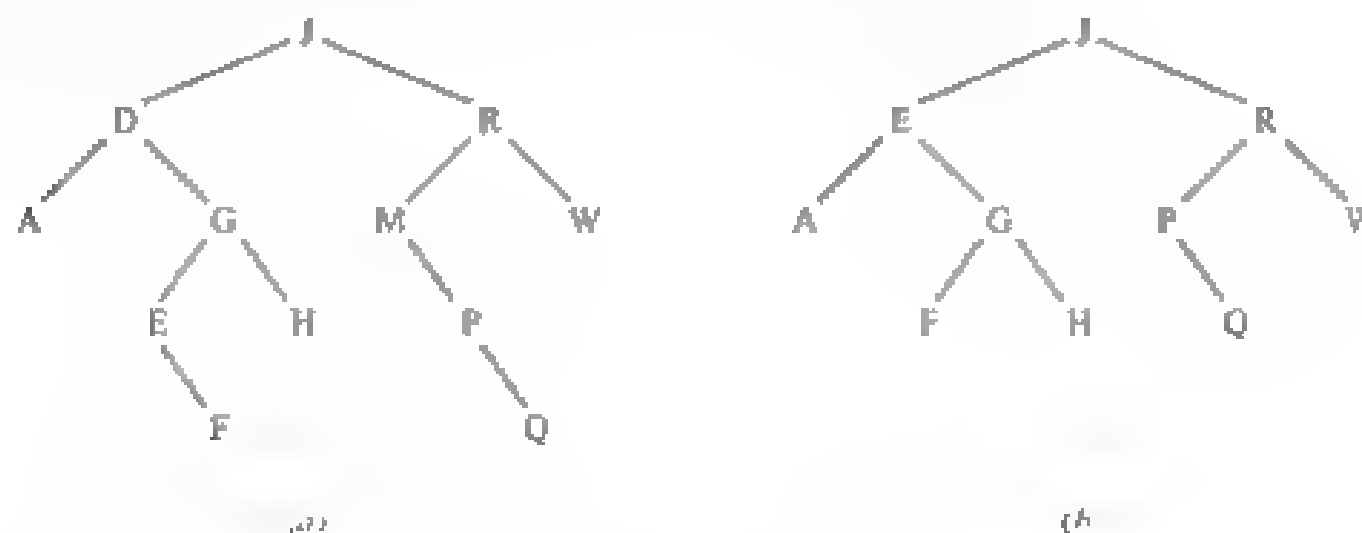



Figura 10-28

(b) O percurso inordem de *T* é o que se segue.

$$A, D, E, F, G, H, J, M, P, Q, R, W$$

Observe que essa é a listagem alfabética das letras. (O percurso inordem de qualquer árvore binária de busca *T* conduz a uma lista ordenada dos nós.)

10.11 Considere a árvore binária T na Fig. 10-28(a). Descreva a árvore T depois que (a) o nó M e (b) o nó D são deletados.

(a) O nó M tem apenas um filho P. Portanto, delete M e faça P se tornar o filho à esquerda de R no lugar de M.

(b) O nó D tem dois filhos. Encontre o sucessor inordem de D, que é o nó E. Primeiro, delete E da árvore e então substitua D pelo nó E.

A Fig. 10-28(b) mostra a árvore T atualizada.

10.12 Seja H o heap mínimo na Fig. 10-29(a). (H é um heap mínimo, uma vez que os elementos menores estão no topo do heap, em vez dos maiores.) Descreva o heap depois que ITEM = 11 é inserido em H.

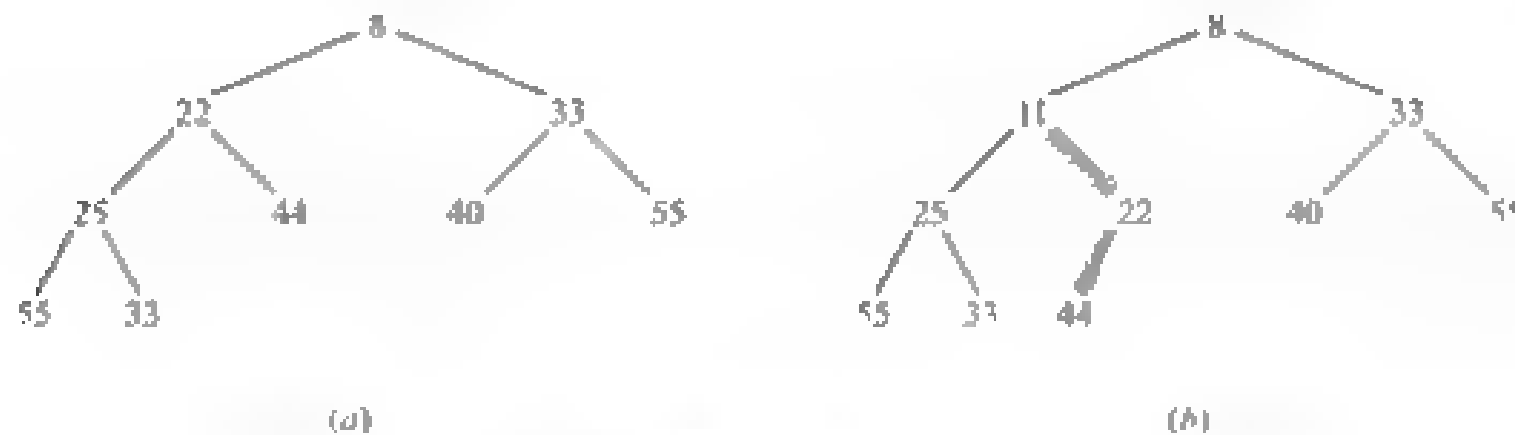



Figura 10-29

Primeiro, insira ITEM como o próximo nó da árvore completa, isto é, como o filho à esquerda do nó 44. Em seguida, compare repetidamente ITEM com seu PAI e permute ITEM e PAI enquanto ITEM < PAI. Como 11 < 44, permute 11 e 44. Como 11 < 22, permute 11 e 22. Como 11 > 8, ITEM = 11 encontrou seu lugar apropriado no heap H. A Fig 10-29(b) mostra o heap final H. As arestas sombreadas indicam o caminho de ITEM à medida que ele se move sobre a árvore.

Comprimento de caminho, algoritmo de Huffman

10.13 Seja T a 2-árvore ponderada na Fig. 10-30(a). Determine o comprimento do caminho ponderado P da árvore T.

Multiplique cada peso W pelo comprimento L, do caminho da raiz de T para o nó contendo o peso e, então, some todos esses produtos para obter P. Assim:

$$\begin{aligned} P &= 4(2) + 15(4) + 25(4) + 5(3) + 8(2) + 16(2) \\ &= 8 + 60 + 100 + 15 + 16 + 32 \\ &= 231 \end{aligned}$$

10.14 Suponha que seis pesos, 4, 15, 25, 5, 8, 16, sejam dados. Encontre uma 2-árvore T com os pesos dados e com um comprimento de caminho P mínimo. (Compare T com a árvore da Fig. 10-30(a).)

Use o algoritmo de Huffman. Ou seja, combine repetidamente as duas subárvores com pesos mínimos em uma única subárvore como se segue:

(a) 4, 15, 25, 5, 8, 16;
(b) 15, 25, (9), 8, 16;
(c) 15, 25, (17), 16;
(d) 25, 17, (31);
(e) (42), 31,
(f) (73)

(O número circulado indica a raiz da nova subárvore no passo.) A árvore T é esboçada a partir do passo (f) para trás, conduzindo à Fig. 10-30(b). O comprimento do caminho de T se segue:

$$\begin{aligned} P &= 25(2) + 4(4) + 5(4) + 8(3) + 15(2) + 16(2) \\ &= 50 + 16 + 20 + 24 + 30 + 32 \\ &= 172 \end{aligned}$$

(A árvore da Fig. 10-30(a) tem comprimento de caminho 231.)

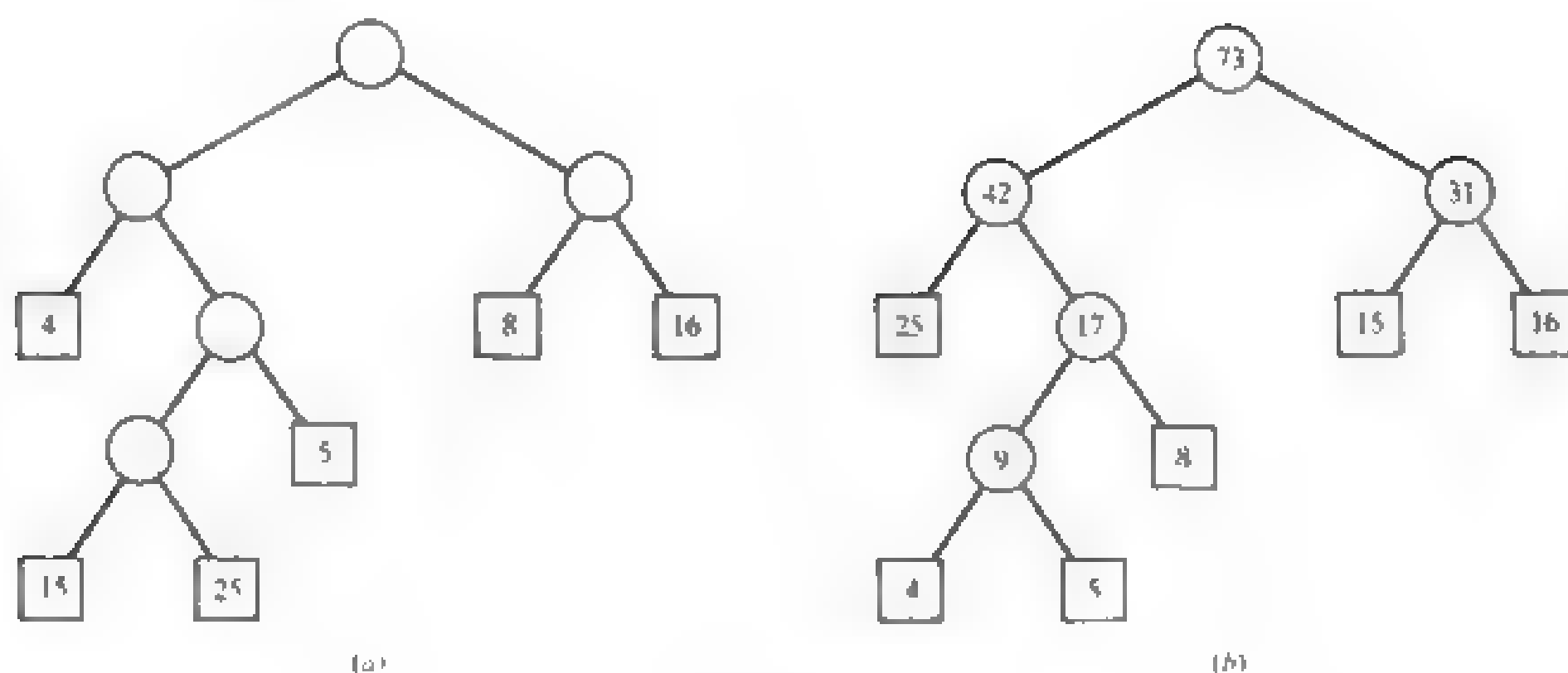



Figura 10-30

10.15 Suponha que itens de dados A, B, C, D, E, F, G ocorram com a seguinte distribuição de probabilidades.

Itens de dados:	A	B	C	D	E	F	G
Probabilidade:	10	30	5	15	20	15	5

Encontre um código de Huffman para os itens de dados.

Como na Fig. 10-31(a), aplique o algoritmo de Huffman para econtrar uma 2-árvore com comprimento de caminho ponderado mínimo P. (Novamente o número circulado indica a raiz da nova subárvore no passo.) A árvore T é esboçada a partir do passo (g) para trás, levando à Fig. 10-31(b). Assinale rótulos de bit às arestas da árvore T, 0 para uma aresta à esquerda e 1 para uma aresta à direita, como na Fig. 10-31(b). A árvore T nos leva ao seguinte código de Huffman

$$A{:}000; \quad B{:}11; \quad C{:}0010; \quad D{:}100; \quad E{:}01; \quad F{:}101; \quad G{:}0011$$

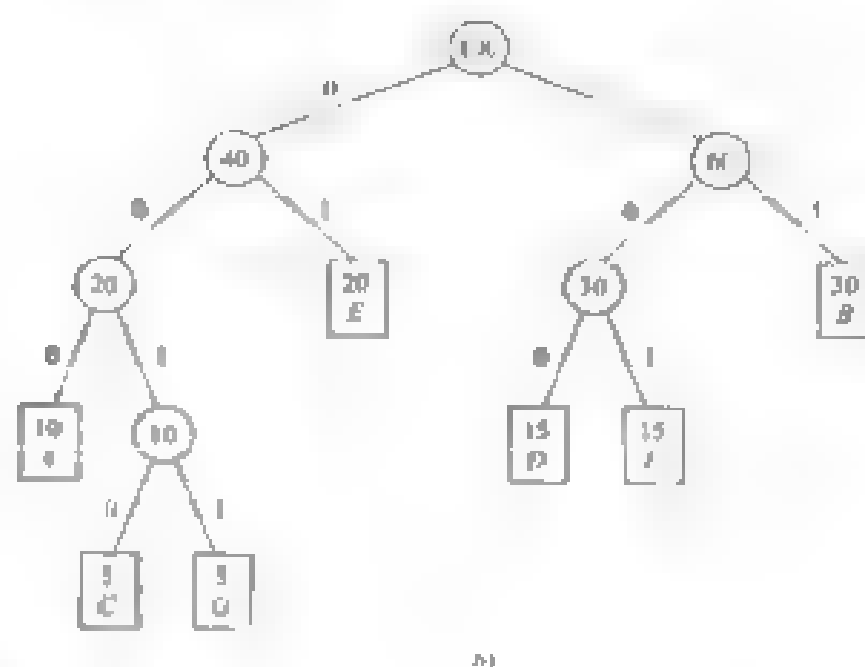
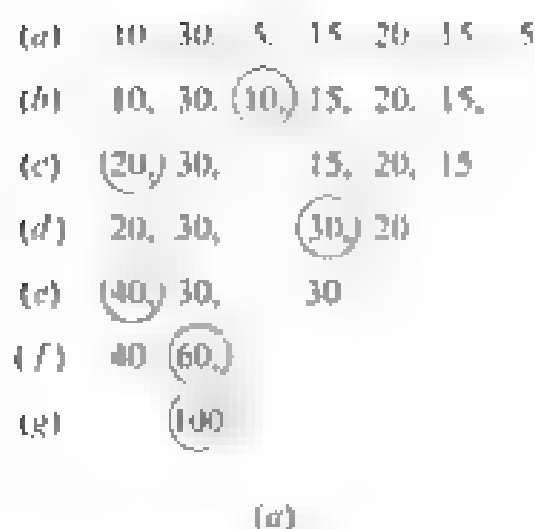



Figura 10-31

Árvores gerais

10.16 Seja T a árvore geral da Fig. 10-32(a). Encontre a árvore binária T' correspondente.

Os nós de T' são os mesmos nós da árvore geral T. Em particular, a raiz de T' é a mesma de T. Além disso, se N é um nó na árvore binária T', então seu filho à esquerda é o primeiro filho de N em T, e seu filho à direita é o próximo irmão de N em T. Construindo T' a partir da raiz, para baixo, obtemos a árvore da Fig. 10-32(b).

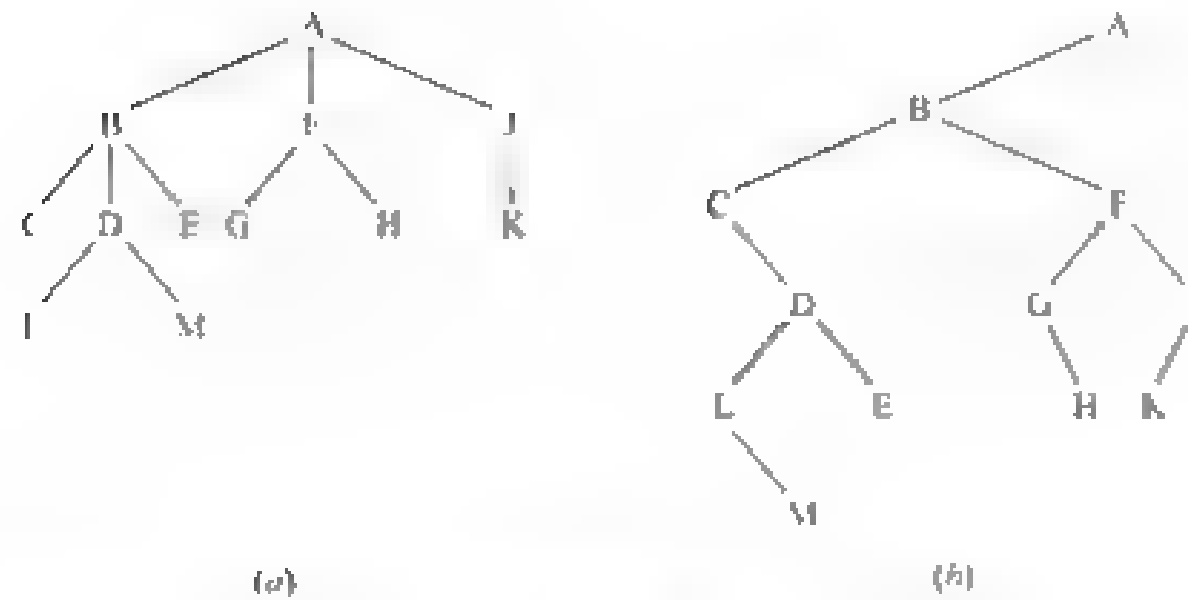



Figura 10-32

Problemas Complementares

10.17 Considere a árvore binária *T* na Fig. 10-33(*a*).

(a) Encontre: (i) a profundidade *d* de *T*; (ii) os descendentes de *B*.

(b) Percorra *T* em: (i) pré-ordem, (ii) inordem; (iii) pós-ordem.

(c) Encontre os nós terminais de *T* e as ordens em que eles são percorridos em (b).

10.18 Repita o Problema 10.17 para a árvore binária *T* na Fig. 10-33(*b*).

10.19 Repita o Problema 10.17 para a árvore binária *T* na Fig. 10-33(*c*).

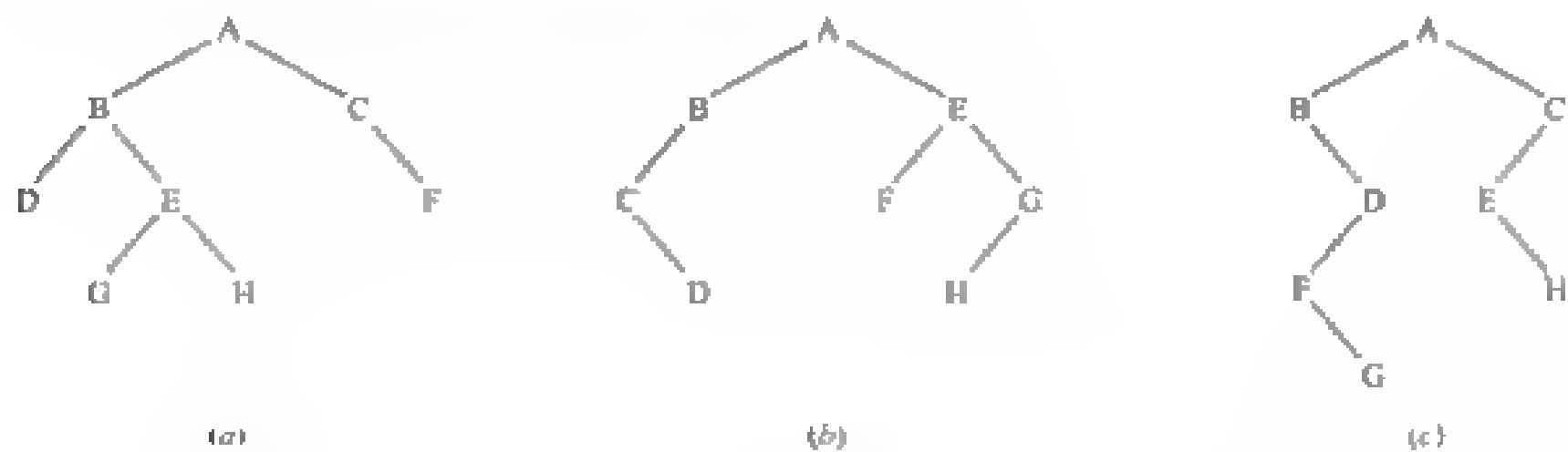



Figura 10-33

10.20 Seja *T* a árvore binária armazenada na memória, como na Fig. 10-34, onde ROOT = 14.

(a) Esboce o diagrama de *T*.

(b) Percorra *T* em: (i) pré-ordem, (ii) inordem; (iii) pós-ordem.

(c) Determine a profundidade *d* de *T*

(d) Encontre o número mínimo de localizações exigidas para um array linear TREE se *T* fosse armazenada sequencialmente em TREE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
INFO	*H*	*K*		*P*	*B*		*E*		*C*	*F*	*Q*	*S*		*J*	*A*	*L*		*D*
LEFT	4	0		0	18		1		0	15	0	0		5	2	0		0
RIGHT	11	0		0	7		0		0	16	12	6		9	0	0		0

Figura 10-34

10.21 Suponha que os percursos pré-ordem e inordem de uma árvore binária T resultem nas seguintes sequências de nós.

Pré-ordem:	G,	B,	Q,	A,	C,	K,	F,	P,	D,	E,	R,	H
Inordem:	Q,	B,	K,	C,	F,	A,	G,	P,	E,	D,	H,	R

(a) Esboce o diagrama de T.

(b) Encontre: (i) a profundidade d de T; (ii) descendentes de B

(c) Liste os nós terminais de T.

10.22 Considere a expressão algébrica $E = (x + 3y)^4(a - 2b)$. (a) Esboce a 2-árvore correspondente. (b) Escreva E na forma prefixa polonesa.

Árvores de busca binárias, heaps

10.23 Encontre a árvore final T se os seguintes números são inseridos em uma árvore binária vazia de busca T:

50, 33, 44, 22, 77, 35, 60, 40

10.24 Encontre o heap final H se os números do Problema 10.23 são inseridos em um heap máximo vazio H.

10.25 Encontre o heap final H se os números do Problema 10.23 são inseridos em um heap mínimo vazio H.

10.26 Seja T a árvore binária de busca na Fig. 10-35(a). Suponha que os nós 20, 55 e 88 são adicionados, um após o outro, a T. Determine a árvore final T.

10.27 Seja T a árvore binária de busca na Fig. 10-35(a). Suponha que os nós 22, 25 e 75 são adicionados, um após o outro, a T. Determine a árvore final T.

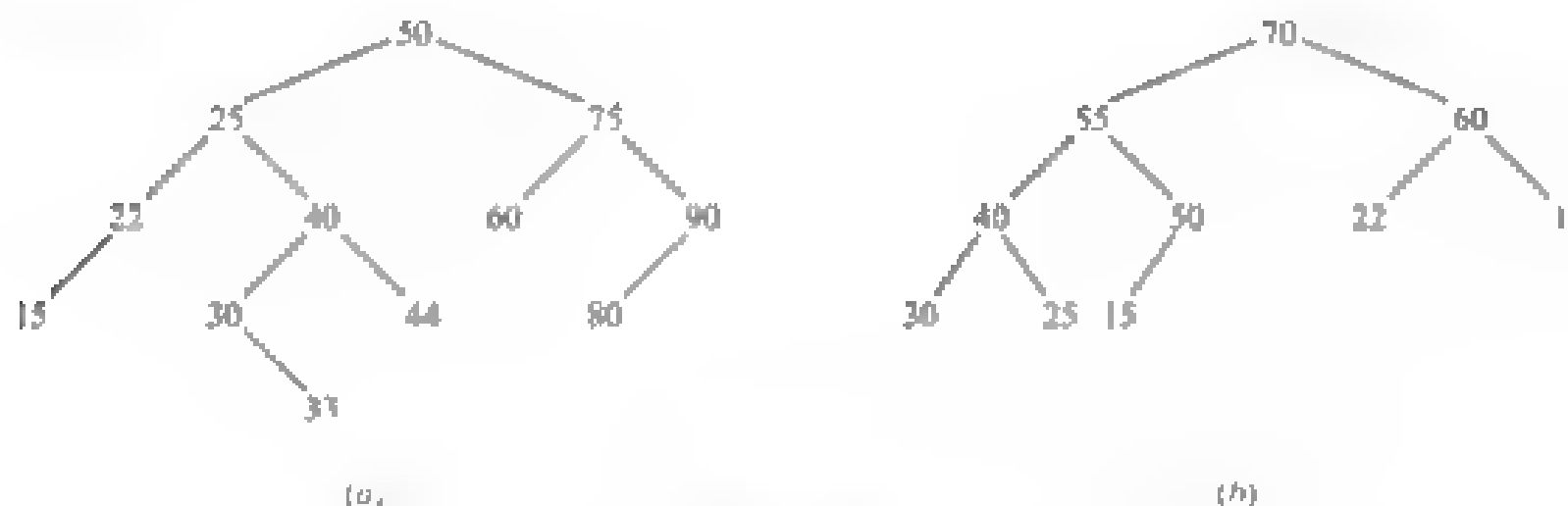



Figura 10-35

10.28 Seja H o heap na Fig. 10-35(b). Encontre o heap final H se os números 65, 44 e 75 são inseridos, um após o outro, em H.

10.29 Seja H o heap na Fig. 10-35(b). Determine o heap final H se a raiz e depois a próxima raiz são deletadas de H.

Algoritmo de huffman, árvores gerais

10.30 Considere a 2-árvore T na Fig. 10-36(a), a qual contém as letras A, B, C, D, E, F, G como nós externos. Encontre a codificação de Huffman das letras, determinada pela árvore T.

10.31 Encontre o comprimento de caminho ponderado P da árvore na Fig. 10-36(a) se os itens de dados A, B, ..., G são assinalados aos seguintes pesos:

$(A, 13), (B, 2), (C, 19), (D, 23), (E, 29), (F, 5), (G, 9)$

10.32 Usando os dados do Problema 10.31, encontre uma codificação de Huffman para as sete letras, usando uma 2-árvore com um comprimento de caminho P mínimo, e determine P.

10.33 Seja T a árvore geral na Fig. 10-36(*b*). Encontre a árvore binária T' correspondente.

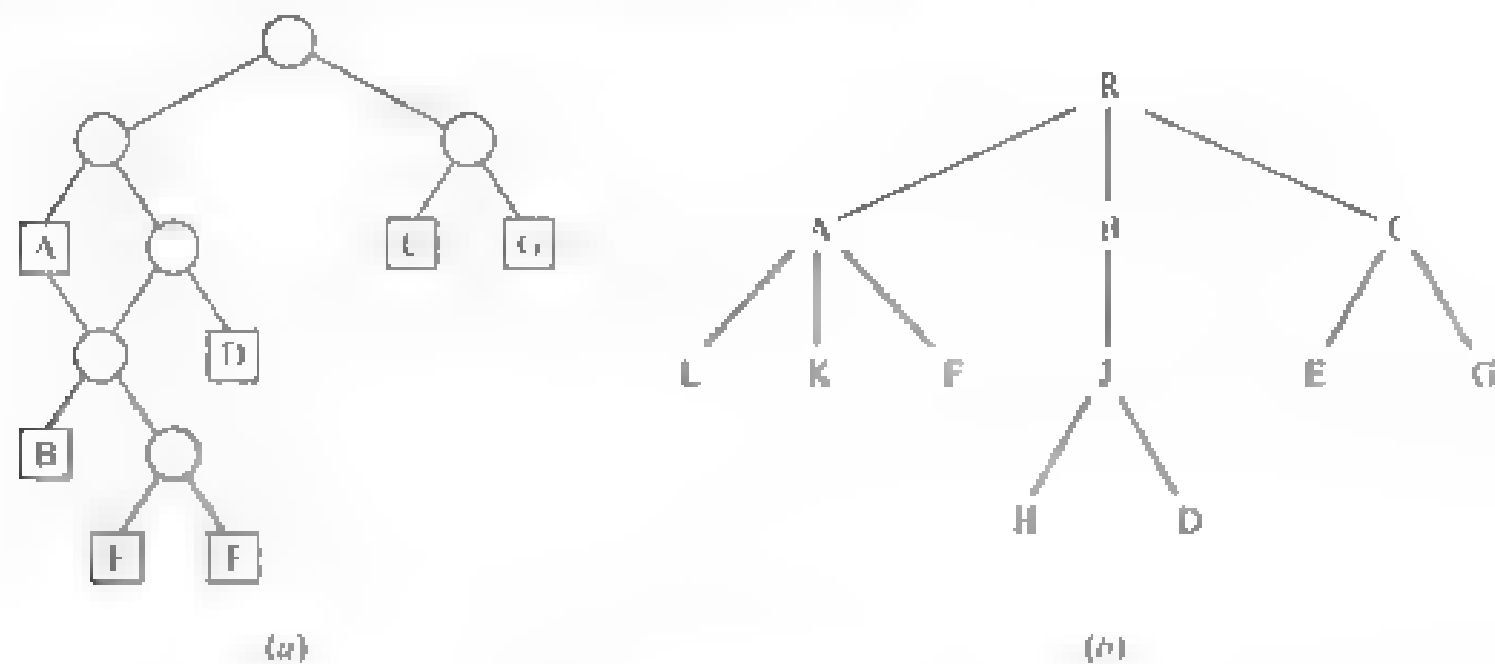



Figura 10-36

Problemas computacionais

Os Problemas 10.34 a 10.40 se referem à Fig. 10-37, que é uma lista de registros de funcionários na memória. Trata-se de uma árvore binária de busca relacionada à chave NAME. Ela usa um apontador HEAD, onde os números de segurdade social dos funcionários+ estão em SSN[HEAD], o salário anual bruto está em SALARY[HEAD] e a raiz da árvore está em LEFT[HEAD]. Além disso, para permitir inserções, as localizações (vazias) disponíveis formam uma lista ligada com AVAIL apontando para o primeiro elemento da lista, e a ligação é mantida pelo array LEFT.

	NAME	SSN	SEX	SALARY	LEFT	RIGHT
1					[illegible]	
2	[illegible]	[illegible]	Feminino	[illegible]	0	12
3	Kelly	[illegible]	Masculino	[illegible]	0	0
4	[illegible]	[illegible]	Masculino	[illegible]	2	0
5		[illegible]		[illegible]	14	0
6	Brown	[illegible]	Feminino	[illegible]	0	0
7	[illegible]	[illegible]	Feminino	[illegible]	3	10
8					11	
9	Cohen	177-44-4557	Masculino	19 000	6	4
10	Rubin	135-46-6262	Feminino	15 500	0	0
11					13	
12	Evans	168-56-8113	Masculino	34 200	0	0
13					1	
14	Harris	208-56-1654	Feminino	22 800	9	7

Figura 10-37

10.34 Desenhe um diagrama da árvore binária de busca NAME.

10.35 Escreva um programa que imprima a lista de registros de funcionários em ordem alfabética. (*Sugestão:* Imprima os registros em inordem.)

10.36 Escreva um programa que leia o nome *NNN* de um funcionário e imprima seu resgistro. Teste o programa usando (a) Evans; (b) Smith, e (c) Lewis.

10.37 Escreva um programa que leia o número de segurdade social *SSS* de um funcionário e imprima o registro dele. Teste o programa usando (a) 165-64-3351; (b) 135-46-626, e (c) 177-44-5555.

+ N. de T. O texto original é norte-americano. Os números de segurdade social nos EUA são equivalentes ao nosso CPF.

10.38 Escreva um programa que leia um inteiro K e imprima o nome de cada funcionário quando $K = 1$ ou de cada funcionária quando $K = 2$. Teste o programa usando: (a) $K = 2$, (b) $K = 5$; e (c) $K = 1$

10.39 Escreva um programa que leia o registro de um novo funcionário e insira o registro no arquivo. Teste o programa usando.

(a) Fletcher; 168-52-3388, Feminino; 21000,

(b) Nelson; 175-32-2468; Masculino; 19000.

Respostas dos Problemas Complementares

10.17 (a) 4, *D, E, G, H*; (b) *ABDEGHCF*, *DBGEHACF*, *DGHEBFCA*; (c) as três: *D, G, H, F*

10.18 (a) 4, *C, D*; (b) *ABCDEFGH*, *CDBAFEHG*, *DCBFHGEA*, (c) as três: *D, F, H*

10.19 (a) 5; *D, F, G*; (b) *ABDFGCEH*, *BFGDAEHC*, *GFDBHECA*; (c) as três. *G, H*

10.20 (a) Ver Fig 10-38(a); (b) *ABDEHPQSCFKRL*, *DBPHQSEACRKFL*, *DPSQHEBRKLFCA*, (c) $d = 6$; logo, $32 \leq$ END $= 64$; aqui END $= 43$.

10.21 (a) Ver Fig. 10-38(b); (b) 5; *QACKF*; (c) *Q, K, F, E, H*.

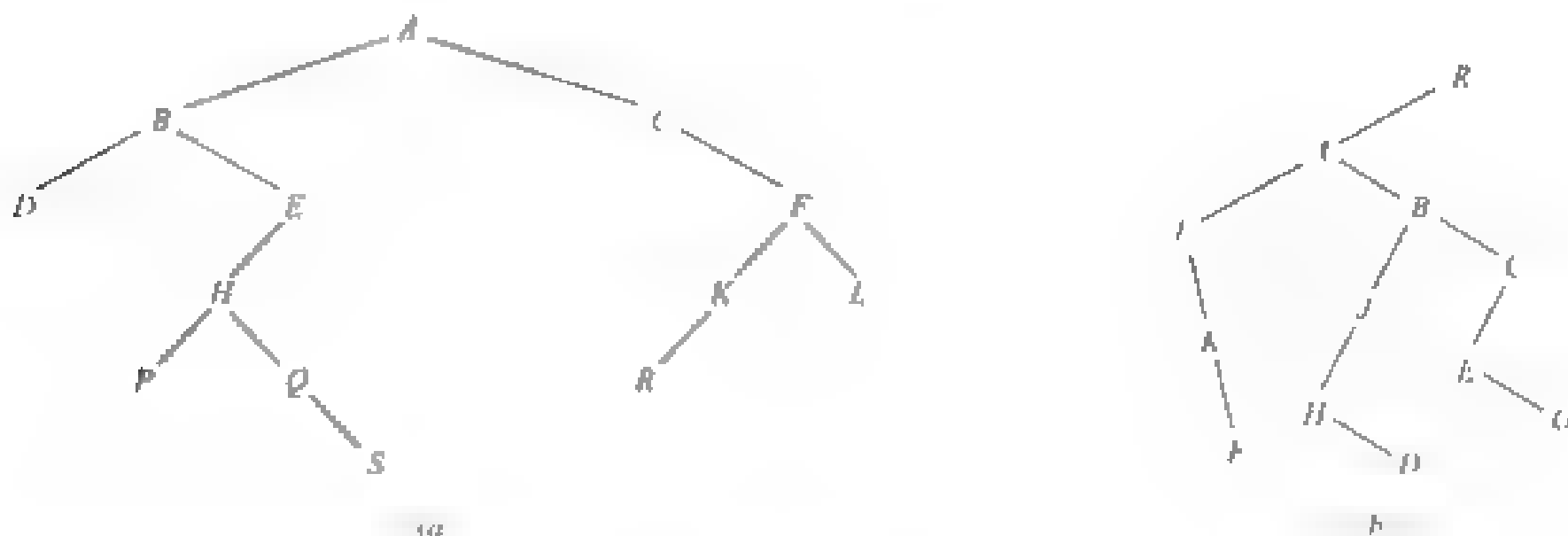



Figura 10-38

10.22 (a) Ver Fig 10-39(a); (b) $* \uparrow + x * 3y4 - a * 2b$

10.23 Ver Fig. 10-39(b).

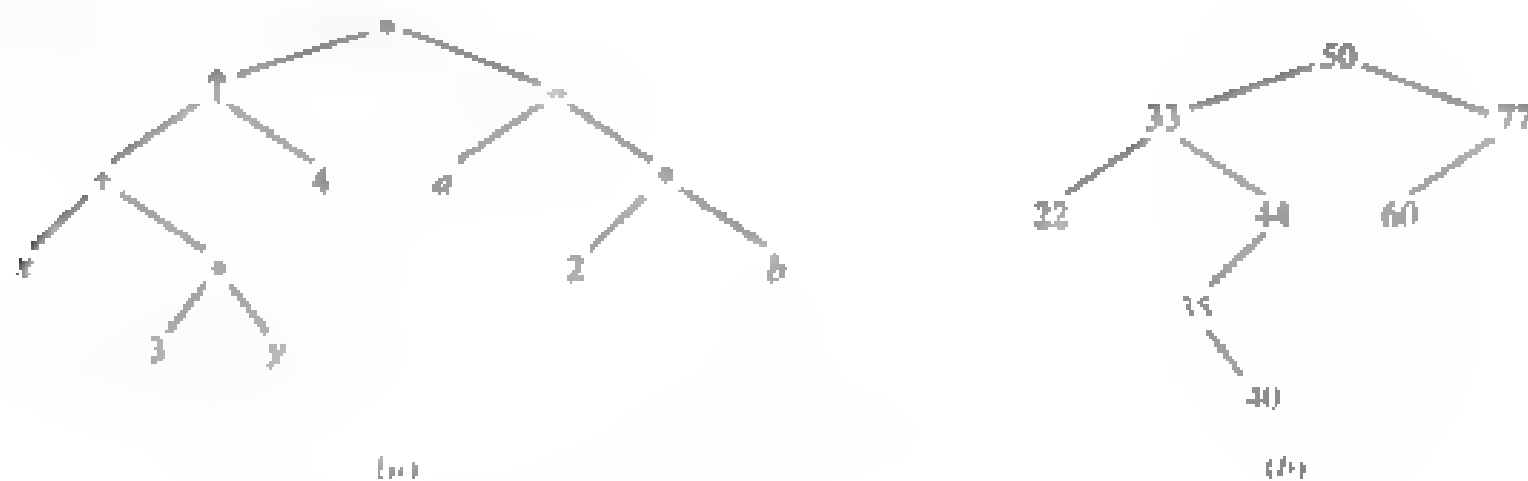



Figura 10-39

10.24 Nível por nível. 77, 50, 60, 40, 33, 35, 44, 22.

10.25 Nível por nível: 22, 33, 35, 40, 77, 44, 60, 50.

10.26 Ver Fig. 10-40(*a*).

10.27 Ver Fig. 10-40(*b*).

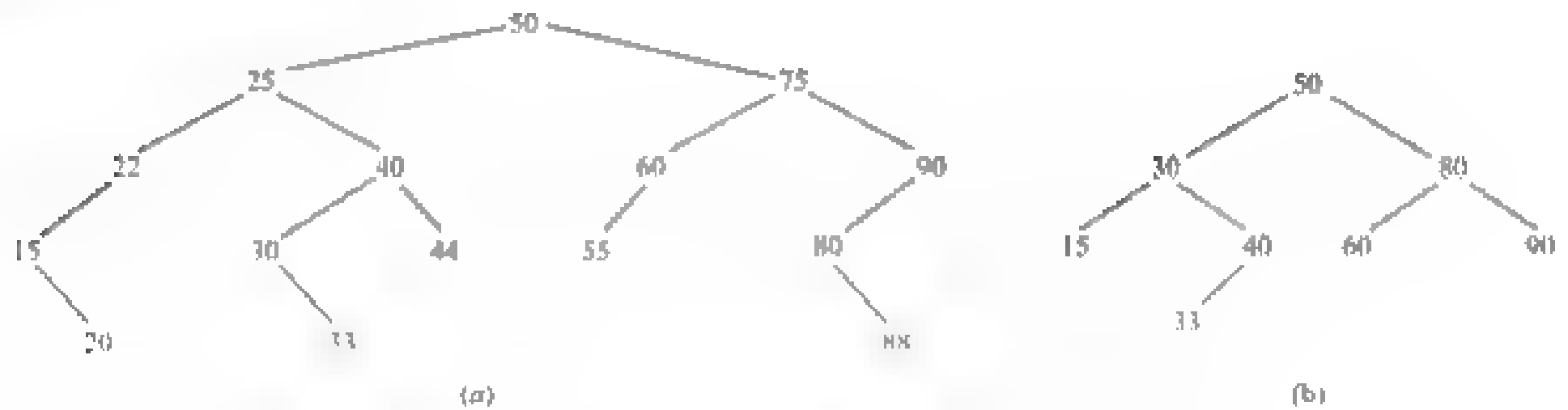



Figura 10-40

10.28 Nível por nível: 75, 65, 70, 40, 55, 60, 11, 30, 25, 15, 50, 22, 44.

10.29 Nível por nível: 55, 50, 22, 40, 25, 15, 11, 30.

10.30 *A*: 00; *B*: 0100; *C*: 10; *D*: 011; *E*: 01010; *F*: 01011; *G*: 11.

10.31 $P = 329$.

10.32 *A*: 000; *B*: 00101, *C*: 10; *D*: 11; *E*: 01; *F*: 00100, *G*: 0011; $P = 257$.

10.33 Ver Fig. 10-41(*a*).

10.34 Ver Fig. 10-41(*b*), onde apenas a primeira letra de cada nome é usada.

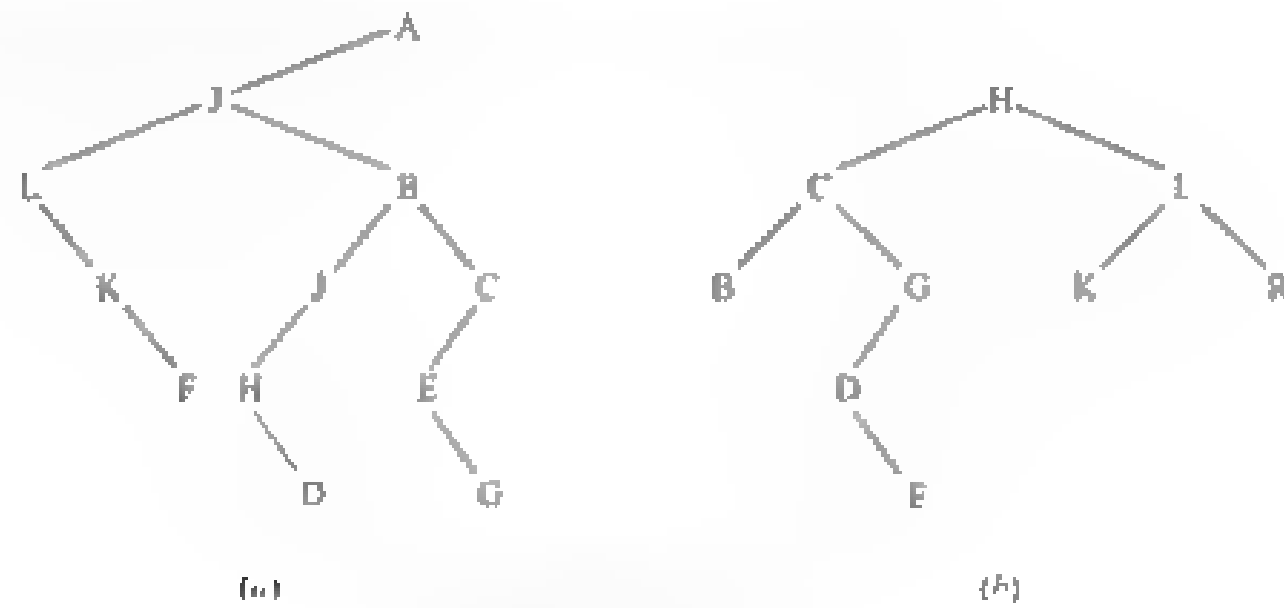



Figura 10-41

Propriedades dos Inteiros

11.1 INTRODUÇÃO

Este capítulo investiga algumas propriedades básicas dos *números naturais* (ou *inteiros positivos*), ou seja, o conjunto

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

bem como seus "primos", os inteiros, isto é, o conjunto

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

(A letra **Z** vem da palavra "Zahlen" que significa "números" em alemão.)

As seguintes regras simples relativas à adição e multiplicação desses números são assumidas (onde a, b e c são inteiros arbitrários):

(a) Lei associativa para multiplicação e adição:

$$(a + b) + c = a + (b + c) \text{ e } (ab)c = a(bc)$$

(b) Lei comutativa para multiplicação e adição:

$$a + b = b + a \text{ e } ab = ba$$

(c) Lei distributiva:

$$a(b + c) = ab + ac$$

(d) Identidade da adição 0 e identidade da multiplicação 1:

$$a + 0 = 0 + a = a \text{ e } a \cdot 1 = 1 \cdot a = a$$

(e) Inverso aditivo $-a$ para qualquer inteiro a

$$a + (-a) = (-a) + a = 0$$

O Apêndice **B** mostra que outras estruturas matemáticas têm as propriedades acima. Uma propriedade fundamental que diferencia os inteiros **Z** de outras estruturas é o Princípio de Indução Matemática (Seção 1.8), o qual novamente discutimos aqui. Também estabelecemos e provamos (Problema 11.30) o seguinte teorema.

Teorema Fundamental da Aritmética: Todo inteiro positivo $n > 1$ pode ser escrito univocamente como um produto entre números primos.

Esse teorema já apareceu nos *Elementos* de Euclides. Aqui também desenvolvemos os conceitos e métodos que são empregados para demonstrar tão importante teorema.

11.2 ORDEM E DESIGUALDADES, VALOR ABSOLUTO

Esta seção discute as propriedades elementares de ordem e valor absoluto.

Ordem

Observe que definimos ordem em **Z** em termos dos inteiros positivos **N**. Todas as propriedades usuais dessa relação de ordem são uma consequência das duas propriedades a seguir de N:

[$\mathbf{P}_1$] Se a e b pertencem a N, então $a + b$ e ab pertencem a N.

[$\mathbf{P}_2$] Para qualquer inteiro a, $a \in \mathbf{N}$, $a = 0$ ou $-a \in \mathbf{N}$.

A seguinte notação também é utilizada:

$a > b$ significa que $b < a$;	lê-se: a é maior do que b.
$a \leq b$ significa que $a < b$ ou $a = b$;	lê-se: a é menor ou igual a b.
$a \geq b$ significa que $b \geq a$;	lê-se: a é maior ou igual a b.

As relações $<$, $>$, $\leq$ e $\geq$ são chamadas de desigualdades, a fim de distingui-las da relação $=$ de igualdade. O leitor certamente está familiarizado com a representação dos inteiros como pontos em uma reta, conhecida como *reta numérica* **R**, como mostrado na Fig. 11-1.

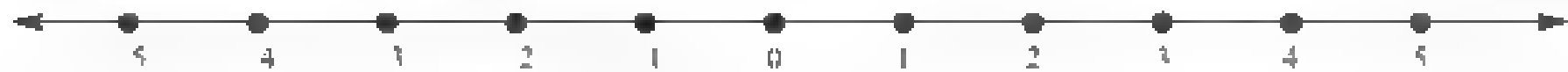



Figura 11-1

Notamos que $a < b$ se, e somente se, a está à esquerda de b na reta numérica **R** da Fig. 11-1. Por exemplo,

$$2 < 5,\ -6 < -3,\ 4 < 4,\ 5 > -8;\ 6 \geq 0;\ -7 \leq 0$$

Observamos também que a é positivo sss $a > 0$ e a é negativo sss $a < 0$. (Lembre que "sss" significa "se, e somente se,".) Propriedades básicas das relações de desigualdade são as que se seguem.

Proposição 11.1: A relação $\leq$ em **Z** tem as seguintes propriedades:

(i) $a \leq a$, para qualquer inteiro a.

(ii) Se $a \leq b$ e $b \leq a$, então $a = b$.

(iii) Se $a \leq b$ e $b \leq c$, então $a \leq c$.

Proposição 11.2 (Lei da Tricotomia): Para quaisquer inteiros a e b, exatamente uma das fórmulas abaixo vale:

$$a < b, \quad a = b \quad \text{ou} \quad a > b$$

Proposição 11.3: Suponha que $a \leq b$ e seja c um inteiro qualquer. Então:

(i) $a + c < b + c$

(ii) $ac \leq bc$ quando $c > 0$; mas $ac \geq bc$ quando $c < 0$.

(O Problema 11.5 demonstra a Proposição 11.3.)

Valor absoluto

O *valor absoluto* de um inteiro a, denotado por $|a|$, é formalmente definido como

$$|a| = \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0 \end{cases}$$

Logo, $|a| > 0$ exceto quando $a = 0$. Em termos geométricos, $|a|$ pode ser percebido como a distância entre os pontos a e 0 sobre a reta numérica **R**. Além disso, $|a - b| = |b - a|$ pode ser vista como a distância entre os pontos a e b. Por exemplo:

$$\text{(a) } |-3| = 3;\ |7| = 7,\ |-13| = 13; \qquad \text{(b) } |2 - 7| = |-5| = 5,\ |7 - 2| = |5| = 5$$

Algumas propriedades da função valor absoluto são as que se seguem. (Os Problemas 11.6 e 11.7 provam (iii) e (iv).)

Proposição 11.4: Sejam a e b quaisquer inteiros. Então:

(i) $|a| \geq 0$, e $|a| = 0$ sss $a = 0$
(ii) $-|a| \leq a \leq |a|$
(iii) $|ab| = |a||b|$
(iv) $|a \pm b| \leq |a| + |b|$
(v) $||a| - |b|| \leq |a \pm b|$

11.3 INDUÇÃO MATEMÁTICA

O Princípio de Indução Matemática dado abaixo, essencialmente, estabelece que os inteiros positivos **N** começam com o número 1 e os demais são obtidos, adicionando sucessivamente 1. Ou seja, começamos com 1, depois $2 = 1 + 1$, em seguida, $3 = 2 + 1$, então $4 = 3 + 1$, e assim por diante. O princípio torna precisa a expressão "e assim por diante".

Princípio de Indução Matemática: Seja S um conjunto de inteiros positivos com as duas propriedades a seguir

(i) 1 pertence a S.
(ii) Se k pertence a S, então $k + 1$ pertence a S.

Então S é o conjunto de todos os inteiros positivos.

Não provamos tal princípio. Ao contrário, quando o conjunto **N** de inteiros positivos (números naturais) é desenvolvido axiomaticamente, esse princípio é dado como um dos axiomas.†

Existe uma forma equivalente do princípio acima que é usualmente empregada quando se demonstra teoremas:

Princípio de Indução Matemática: Seja P uma proposição definida sobre os inteiros $n \geq 1$, tal que

(i) $P(1)$ é verdadeira.
(ii) $P(k + 1)$ é verdadeira sempre que $P(k)$ for verdadeira.

Então P é verdadeira para todo inteiro $n \geq 1$.‡

Exemplo 11.1

(a) Seja P a proposição de que a soma dos primeiros n números ímpares é n^2, ou seja.

$$P(n)\text{: } 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

(O n-ésimo número ímpar é $2n - 1$ e o próximo número ímpar é $2n + 1$.)

† N. de T. O leitor deve ser cuidadoso com essa afirmação dos autores. Qualquer axioma em qualquer teoria formal axiomática é demonstrável. Ver, por exemplo, *Introduction to Mathematical Logic*, de E. Mendelson, ou *O que é um Axioma*, de A. S. Sant'Anna.

‡ N. de T. Aqui, e ao longo do texto, os autores implicitamente consideram que todo teorema é verdadeiro e que toda fórmula verdadeira é teorema. Rigorosamente isso é falso. Mas, para os propósitos do livro, é uma hipótese tolerável.

Claramente, $P(n)$ é verdadeira para $n = 1$; isto é:

$$P(1).\ 1 = 1^2$$

Suponha que $P(k)$ é verdadeira. (Essa é chamada de hipótese indutiva.) Adicionando $2k + 1$ em ambos os lados de $P(k)$, obtemos

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) &= k^2 + (2k + 1) \\ &= (2k + 1)^2 \end{aligned}$$

que é $P(k + 1)$. Mostramos que $P(k + 1)$ é verdadeira sempre que $P(k)$ for verdadeira. Pelo Princípio de Indução Matemática, P é verdadeira para todos os inteiros positivos n.

(b) O símbolo $n!$ (lê-se: n fatorial) é definido como o produto dos primeiros n inteiros positivos, isto é.

$$1! = 1,\ 2! = 2 \cdot 1 = 2,\ 3! = 3 \cdot 2 \cdot 1 = 6, \text{ e assim por diante.}$$

Isso pode ser formalmente definido como se segue.

$$1! = 1 \text{ e } (n + 1)! = (n + 1)(n!), \text{ para } n > 1$$

Observe que se S é o conjunto de inteiros positivos para os quais ! é definida, então S satisfaz as duas propriedades de indução matemática. Logo, a definição acima caracteriza ! para todo inteiro positivo.

Existe outra forma do Princípio de Indução Matemática (provada no Problema 11.13) que é, às vezes, mais conveniente usar, a saber:

Teorema 11.5 (indução: segunda forma): Seja P uma proposição definida sobre os inteiros $n \geq 1$ tal que:

(i) $P(1)$ é verdadeira.

(ii) $P(k)$ é verdadeira sempre que $P(j)$ é verdadeira para todo $1 \leq j < k$.

Então P é verdadeira para todo inteiro $n \geq 1$.

Observação: O teorema acima é verdadeiro se substituirmos 1 por 0 ou por qualquer outro inteiro a.

Princípio da boa ordem

Uma propriedade dos inteiros positivos que é equivalente ao princípio de indução, apesar de ser aparentemente muito diferente, é o Princípio da Boa Ordem (demonstrado no Problema 11.12), a saber:

Teorema 11.6 (Princípio da Boa Ordem): Seja S um conjunto não vazio de inteiros positivos. Então S contém um *menor elemento*, ou seja, S contém um elemento a tal que $a \leq s$ para todo s em S

Em termos gerais, um conjunto ordenado S é dito *bem-ordenado* se todo subconjunto de S contém um primeiro elemento. Assim, o Teorema 11.6 estabelece que $\mathbf{N}$ é bem-ordenado.

Um conjunto S de inteiros é dito *cotado inferiormente* se todo elemento de S é maior do que algum inteiro m (que pode ser negativo). (O número m é chamado de *cota inferior* de S.) Um corolário simples do teorema acima é o que se segue:

Corolário 11.7: Seja S um conjunto não vazio de inteiros que é cotado inferiormente. Então S contém um menor elemento.

11.4 ALGORITMO DA DIVISÃO

A propriedade fundamental a seguir da aritmética (demonstrada nos Problemas 11.17 e 11.18) é essencialmente uma outra forma do resultado da divisão longa.

Teorema 11.8 (algoritmo da divisão): Sejam a e b inteiros com $b \neq 0$. Então existem inteiros q e r tais que

$$a = bq + r \text{ e } 0 \leq r < |b|$$

Além disso, os inteiros q e r são únicos.

O número q no teorema anterior é chamado de *quociente*, e r é chamado de *resto*. Insistimos no fato de que r deve ser não negativo. O teorema também estabelece que

$$r = a - bq$$

Essa equação é usada adiante.

Se a e b são positivos, então q é não negativo. Se b é positivo, então a Fig. 11-2 fornece uma interpretação geométrica desse teorema. Ou seja, os múltiplos positivos e negativos de b são igualmente distribuídos ao longo da reta numérica **R**, e a se encontra entre alguns múltiplos qb e $(q + 1)b$. A distância entre qb e a é então o resto r.

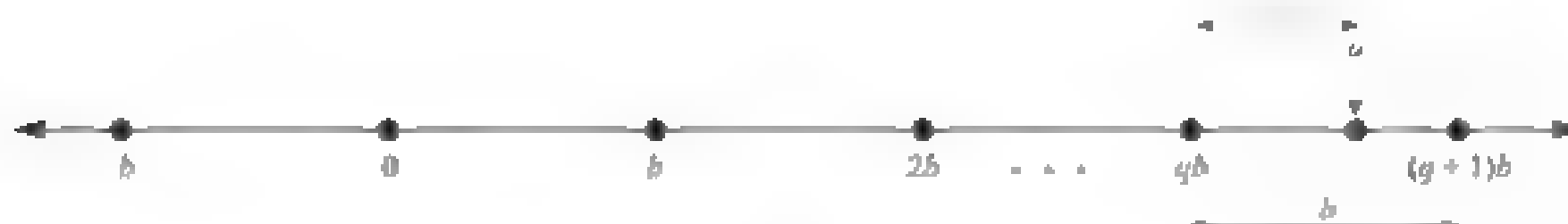



Figura 11-2

Algoritmo da divisão, usando uma calculadora

Suponha que a e b sejam ambos positivos. Então pode-se encontrar o quociente q e o resto r, usando uma calculadora da seguinte maneira:

Passo 1. Divida a por b, usando a calculadora, isto é, encontre a/b.

Passo 2. Seja q a parte inteira de a/b, ou seja, $q = INT(a/b)$.

Passo 3. Seja r a diferença entre a e bq, ou seja, $r = a - bq$.

Exemplo 11.2

(a) Sejam $a = 4461$ e $b = 16$. Podemos descobrir o quociente $q = 278$ e o resto $r = 13$ pela divisão longa. Alternativamente, usando uma calculadora, obtemos q e r como se segue:

$$a/b = 278{,}8125\ldots,\ q = 278,\ r = 4461 - 16(278) = 13$$

Como esperado, $a = bq + r$, logo:

$$4461 = 16(278) + 13$$

(b) Sejam $a = -262$ e $b = 3$. Primeiro, dividimos $|a| = 262$ por $b = 3$. Isso leva ao quociente $q' = 87$ e a um resto $r' = 1$. Logo,

$$262 = 3(87) + 1$$

Precisamos de $a = -262$. Logo, multiplicamos por -1, obtendo

$$-262 = 3(-87) - 1$$

Contudo, -1 é negativo e, portanto, não pode ser r. Corrigimos isso, adicionando e subtraindo o valor de b (que é 3) como se segue:

$$-262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2$$

Então, $q = -88$ e $r = 2$.

(c) Seja $b = 2$. Então, qualquer inteiro a pode ser escrito na forma

$$a = 2q + r, \text{ onde } 0 \leq r < 2$$

Assim, r só pode ser 0 ou 1. Logo, todo inteiro é da forma $2k$ ou $2k + 1$. Os inteiros da forma $2k$ são chamados de *pares*, enquanto aqueles da forma $2k + 1$ são conhecidos como *ímpares*. (Geralmente um inteiro par é definido como um inteiro divisível por 2, enquanto todos os demais são ditos ímpares. Logo, o algoritmo da divisão prova que todo inteiro ímpar tem a forma $2k + 1$.)

11.5 DIVISIBILIDADE, PRIMOS

Sejam a e b inteiros com $a \neq 0$. Suponha que $ac = b$, para algum inteiro c. Dizemos então que a divide b ou b é divisível por a e denotamos isso por

$$a|b$$

Também dizemos que b é um *múltiplo* de a ou que a é um *fator* ou *divisor* de b. Se a não divide b, escrevemos $a \nmid b$.

Exemplo 11.3

(a) Claramente $3 \mid 6$, pois $3 \cdot 2 = 6$, e $-4 \mid 28$, pois $(-4)(-7) = 28$.

(b) Os divisores de 4 são ± 1, ± 2 e ± 4, e os divisores de 9 são ± 1, ± 3 e ± 9.

(c) Se $a \neq 0$, então $a \mid 0$, uma vez que $a \cdot 0 = 0$.

(d) Todo inteiro a é divisível por ± 1 e $\pm a$. Esses são chamados, às vezes, de *divisores triviais* de a. As propriedades básicas de divisibilidade são estabelecidas no próximo teorema (demonstrado no Problema 11.24).

Teorema 11.9: Suponha que a, b e c são inteiros.

(i) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

(ii) Se $a \mid b$, então para qualquer inteiro x, $a \mid bx$.

(iii) Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$ e $a \mid (b - c)$.

(iv) Se $a \mid b$ e $b \neq 0$, então $a = \pm b$ ou $|a| < |b|$.

(v) Se $a \mid b$ e $b \mid a$, então $|a| = |b|$, ou seja, $a = \pm b$.

(vi) Se $a \mid 1$, então $a = \pm 1$.

Colocando (ii) e (iii) juntos, obtemos o seguinte resultado importante.

Corolário 11.10: Suponha que $a \mid b$ e $a \mid c$. Então, para quaisquer inteiros x e y, $a \mid (bx + cy)$. A expressão $bx + cy$ é chamada de *combinação linear* de b e c.

Primos

Um inteiro positivo $p > 1$ é chamado de *número primo* ou *primo* se seus únicos divisores são ± 1 e $\pm p$, isto é, se p admite apenas divisores triviais. Se $n > 1$ não é primo, então n é dito *composto*. Observamos (Problema 11.13) que se $n > 1$ é composto, então $n = ab$, onde $1 < a, b < n$.

Exemplo 11.4

(a) Os inteiros 2 e 7 são primos, enquanto $6 = 2 \cdot 3$ e $15 = 3 \cdot 5$ são compostos.

(b) Os primos menores do que 50 são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

(c) Apesar de 21, 24 e 1729 não serem primos, cada um pode ser escrito como um produto de primos:

$$21 = 3 \cdot 7, 24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3; 1729 = 7 \cdot 13 \cdot 19$$

O Teorema Fundamental da Aritmética estabelece que todo inteiro $n > 1$ pode ser escrito como um produto de primos essencialmente de uma maneira; é um teorema profundo e difícil de demonstrar. Contudo, usando indução, é fácil provar que tal produto existe. Assim:

Teorema 11.11: Todo inteiro $n > 1$ pode ser escrito como um produto de primos.

Note que um produto pode consistir em um único fator, de modo que um primo p é ele mesmo um produto de primos. Demonstramos o Teorema 11.11 aqui, uma vez que sua prova é relativamente simples.

Demonstração: A prova é por indução. Seja $n = 2$. Como 2 é primo, n é um produto de primos. Suponha que $n > 2$ e que o teorema vale para inteiros positivos menores do que n. Se n é primo, então n é um produto de primos. Se n é composto, então $n = ab$, onde $a, b < n$. Por indução, a e b são produtos de primos, logo, $n = ab$ é também um produto de primos.

Euclides, que demonstrou o Teorema Fundamental da Aritmética, também questionou se existe ou não um maior primo. Ele respondeu à questão da seguinte maneira:

Teorema 11.12: Não existe maior primo, ou seja, há uma quantidade infinita de primos.

Demonstração: Suponha que existe um número finito de primos, digamos, $p_1, p_2, \ldots, p_m$. Considere o inteiro

$$n = p_1 p_2 \cdots p_m + 1$$

Como n é um produto de primos (Teorema 11.11), ele é divisível por um dos primos, digamos, p_k. Note que p_k também divide o produto $p_1 p_2 \ldots p_m$. Logo, p_k divide

$$n - p_1 p_2 \cdots p_m = 1$$

Isso é impossível e, assim, n é divisível por algum outro primo. Isso contradiz a hipótese de que $p_1, p_2, \ldots, p_m$ são os únicos primos. Portanto, o número de primos é infinito e o teorema está demonstrado.

11.6 MÁXIMO DIVISOR COMUM, ALGORITMO EUCLIDIANO

Suponha que a e b são inteiros, não sendo o caso de ambos 0. Um inteiro d é chamado de *divisor comum* de a e b se d divide ambos a e b, ou seja, se $d \mid a$ e $d \mid b$. Note que 1 é um divisor comum de a e b e que qualquer divisor comum de a e b não pode ser maior do que $|a|$ ou $|b|$. Assim, existe um maior divisor comum de a e b; ele é denotado por

$$\text{mdc}(a, b)$$

e é chamado de *máximo divisor comum* de a e b.

Exemplo 11.5

(a) Os divisores comuns de 12 e 18 são $\pm 1, \pm 2, \pm 3$ e ± 6. Assim, $\text{mdc}(12, 18) = 6$. Analogamente:

$$\text{mdc}(12, -18) = 16, \text{mdc}(12, -16) = 4, \text{mdc}(29, 15) = 1, \text{mdc}(14, 49) = 7$$

(b) Para qualquer inteiro a, temos $\text{mdc}(1, a) = 1$.

(c) Para qualquer primo p, temos $\text{mdc}(p, a) = p$ ou $\text{mdc}(p, a) = 1$, dependendo se p divide ou não a.

(d) Suponha que a é positivo. Então $a \mid b$ se, e somente se, $\text{mdc}(a, b) = a$.

O teorema a seguir (demonstrado no Problema 11.26) fornece uma caracterização alternativa do máximo divisor comum.

Teorema 11.13: Seja d o menor inteiro positivo da forma $ax + by$. Então

$$d = \text{mdc}(a, b)$$

Corolário 11.14: Suponha que $d = \text{mdc}(a, b)$. Então existem inteiros x e y tais que $d = ax + by$

Outra maneira de caracterizar o máximo divisor comum, sem empregar a relação de desigualdade, é a seguinte.

Teorema 11.15: Um inteiro positivo $d = \text{mdc}(a, b)$ se, e somente se, d tem as duas propriedades a seguir

(1) d divide ambos a e b.

(2) Se c divide ambos a e b, então $c \mid d$.

Propriedades simples do máximo divisor comum são:

(a) $\text{mdc}(a, b) = \text{mdc}(b, a)$.

(b) Se $x > 0$, então $\text{mdc}(ax, bx) = x \cdot \text{mdc}(a, b)$

(c) Se $d = \text{mdc}(a, b)$, então $\text{mdc}(a/d, b/d) = 1$.

(d) Para qualquer inteiro x, $\text{mdc}(a, b) = \text{mdc}(a, b + ax)$.

Algoritmo euclidiano

Sejam a e b inteiros e $d = \text{mdc}(a, b)$. Sempre é possível encontrar d, listando todos os divisores de a e então todos os divisores de b, para depois escolher o maior divisor em comum. A complexidade de tal algoritmo é $f(n) = O(\sqrt{n})$, onde $n = |a| + |b|$. Além disso, não apresentamos método algum para encontrar os inteiros x e y tais que $d = ax + by$.

Esta subseção oferece um procedimento muito eficiente, chamado de algoritmo euclidiano, com complexidade $f(n) = O(\log n)$, para determinar $d = \text{mdc}(a, b)$, aplicando o algoritmo da divisão a a e b e então, repetidamente, aplicando-o a cada novo quociente e resto até obtermos um resto nulo. O último resto não nulo é $d = \text{mdc}(a, b)$.

Depois, damos um algoritmo "revelador" que reverte os passos do euclidiano, para encontrar os inteiros x e y tais que $d = xa + yb$.

Ilustramos os algoritmos com um exemplo.

Exemplo 11.6 Sejam $a = 540$ e $b = 168$. Aplicamos o algoritmo euclidiano a a e b. Esses passos, que repetidamente aplicam o algoritmo da divisão a cada quociente e resto até obtermos resto zero, são ilustrados na Fig. 11-3(a), usando a divisão longa, e também na Fig. 11-3(b), onde as flechas indicam o quociente e o resto no passo seguinte. O último resto não nulo é 12. Logo,

$$12 = \text{mdc}(540, 168)$$

Isso segue do fato de que

$$\text{mdc}(540, 168) = \text{mdc}(168, 36) = \text{mdc}(36, 24) = \text{mdc}(24, 12) = 12$$

Em seguida, encontramos x e y tais que $12 = 540x + 168y$ "revela" os passos acima no algoritmo euclidiano. Especificamente, os três primeiros quocientes na Fig. 11-3 conduzem às seguintes equações.

$$(1)\ 36 = 540 - 3(168), \qquad (2)\ 24 = 168 - 4(36), \qquad (3)\ 12 = 36 - 1(24)$$

A equação (3) nos diz que $d = \text{mdc}(a, b) = 12$ é uma combinação linear de 36 e 24. Agora empregamos as equações anteriores em sentido contrário, para eliminar os outros restos. Ou seja, primeiro usamos a equação (2) para substituir 24 na equação (3) e, assim, podemos escrever 12 como uma combinação linear de 168 e 36 da seguinte maneira:

$$(4)\ 12 = 36 - 1[168 - 4(36)] = 36 - 1(168) + 4(36) = 5(36) - 1(168)$$

(1)	(2)	(3)	(4)
$168\overline{)540}$ = 3, 504, resto 36	$36\overline{)168}$ = 4, 144, resto 24	$24\overline{)36}$ = 1, 24, resto 12	$12\overline{)24}$ = 2, 24, resto 0

(a)

(1) $540 = 3(168) + 36$

(2) $168 = 4(36) + 24$

(3) $36 = 1(24) + 12$

(4) $24 = 2(12) + 0$

(b)

Figura 11-3

Em seguida, usamos a equação (1) para substituir 36 em (4), de modo que podemos escrever 12 como uma combinação linear de 168 e 540 da seguinte maneira.

$$12 = 5[540 - 3(168)] - 1(168) = 5(54) - 15(168) - 1(168) = 5(540) - 16(168)$$

Essa é nossa combinação linear desejada. Em outras palavras, $x = 5$ e $y = -16$.

Mínimo múltiplo comum

Suponha que a e b são inteiros diferentes de zero. Note que $|ab|$ é um múltiplo comum positivo de a e b. Assim, existe um menor múltiplo positivo em comum entre a e b; ele é denotado por

$$\text{mmc}(a, b)$$

e é chamado de ***mínimo múltiplo comum*** de a e b.

Exemplo 11.7

(a) $\text{mmc}(2, 3) = 6$; $\text{mmc}(4, 6) = 12$; $\text{mmc}(9, 10) = 90$.

(b) Para qualquer inteiro positivo a, temos $\text{mmc}(1, a) = a$.

(c) Para qualquer primo p e qualquer inteiro positivo a,

$$\text{mmc}(p, a) = a \text{ ou } \text{mmc}(p, a) = ap$$

dependendo se p divide ou não a.

(d) Suponha que a e b sejam inteiros positivos. Então $a \mid b$ se, e somente se, $\text{mmc}(a, b) = b$.

O próximo teorema fornece uma relação importante entre o máximo divisor comum e o mínimo múltiplo comum.

Teorema 11.16: Suponha que a e b são inteiros não nulos. Então

$$\text{mmc}(a, b) = \frac{|ab|}{\text{mdc}(a, b)}$$

11.7 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Esta seção discute o Teorema Fundamental da Aritmética. Primeiro, definimos números inteiros primos entre si

Inteiros primos entre si

Dois inteiros a e b são ditos *primos entre si* ou *coprimos*, se $\text{mdc}(a, b) = 1$. Consequentemente, se a e b são primos entre si, então existem inteiros x e y tais que

$$ax + by = 1$$

Reciprocamente, se $ax + by = 1$, então a e b são primos entre si.

Exemplo 11.8

(a) Observe que $\text{mdc}(12, 35) = 1$, $\text{mdc}(49, 18) = 1$, $\text{mdc}(21, 64) = 1$, $\text{mdc}(-28, 45) = 1$.

(b) Se p e q são primos distintos, então $\text{mdc}(p, q) = 1$.

(c) Para qualquer inteiro a, temos $\text{mdc}(a, a + 1) = 1$, uma vez que qualquer fator comum de a e $a + 1$ deve dividir a diferença $(a + 1) - a = 1$.

A relação de serem primos entre si é particularmente importante por conta dos resultados a seguir. O primeiro teorema é demonstrado no Problema 11.27. Aqui provamos o segundo teorema.

Teorema 11.17: Suponha que $\text{mdc}(a, b) = 1$ e que ambos a e b dividem c. Então ab divide c.

Teorema 11.18: Suponha que $a \mid bc$ e $\text{mdc}(a, b) = 1$. Então $a \mid c$.

Demonstração: Como $\text{mdc}(a, b) = 1$, existem x e y tais que $ax + by = 1$. Multiplicando por c, leva a:

$$acx + bcy = c$$

Temos $a \mid acx$. Além disso, $a \mid bcy$, pois, por hipótese, $a \mid bc$. Logo, a divide a soma $acx + bcy = c$.

Corolário 11.19: Suponha que um primo p divida o produto ab. Então $p \mid a$ ou $p \mid b$.

Esse corolário (provado no Problema 11.28) é de Euclides; ele é a base de sua demonstração para o Teorema Fundamental da Aritmética.

Teorema Fundamental da Aritmética

O Teorema 11.11 estabelece que todo inteiro positivo é um produto de primos. Podem produtos diferentes de primos resultar no mesmo número? Claramente, podemos rearranjar a ordem dos fatores primos, por exemplo,

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5$$

O Teorema Fundamental da Aritmética (demonstrado no Problema 11.30) diz que essa é a única maneira de dois produtos "diferentes" resultarem no mesmo número. Logo:

Teorema 11.20 (Teorema Fundamental da Aritmética): Todo inteiro $n > 1$ pode ser expresso univocamente (exceto quanto à ordem) como um produto de primos.

Os primos na fatoração de n não precisam ser distintos. Frequentemente, é útil reunir todos os primos iguais. Então n pode ser expresso univocamente na forma

$$n = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$$

onde os m_i são positivos e $p_1 < p_2 < \cdots < p_r$. Essa é chamada de *fatoração canônica* de n.

Exemplo 11.9 Dados $a = 2^4 \cdot 3^3 \cdot 7 \cdot 13$ e $b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 17$, encontre $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$.

(a) Primeiro, encontramos $d = \text{mdc}(a, b)$. Os primos p que aparecem em ambos a e b, 2, 3 e 11, também ocorrem em d, e o expoente de p em d é o menor de seus expoentes em a e b. Assim,

$$d = \text{mdc}(a, b) = 2^3 \cdot 3^2 \cdot 11 = 792$$

(b) A seguir, determinamos $m = \text{mmc}(a, b)$. Aqueles primos p que aparecem em a ou b, 2, 3, 5, 7, 11, 13 e 17, também ocorrem em m, e o expoente de p em m é o maior de seus expoentes em a e b. Logo,

$$m = \text{mmc}(a, b) = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17$$

Estamos tão acostumados a empregar números como se o Teorema Fundamental da Aritmética fosse verdadeiro, que pode parecer não haver necessidade de demonstração. É um tributo a Euclides, o primeiro a demonstrar o teorema, o qual reconheceu a necessidade de prova. Enfatizamos a não trivialidade do teorema dando um exemplo de um sistema de números que não o satisfaz.

Exemplo 11.10 Seja F o conjunto de inteiros positivos da forma $3x + 1$. Logo, F consiste nos números:

$$1, 4, 7, 10, 13, 16, 19, 22, \ldots$$

Note que o produto de dois números em F está também em F, pois:

$$(3x + 1)(3y + 1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1$$

Nossa definição de primos faz perfeitamente sentido em F. A despeito de $4 = 2 \cdot 2$, o número 2 não está em F. Logo, 4 é primo em F, pois 4 não admite fatores, exceto 1 e 4. Analogamente, 10, 22, 25, . . . são primos em F. Listamos os primeiros primos em F:

$$4, 7, 10, 13, 19, 22, 25, \ldots$$

Observe que $100 = 3(33) + 1$ pertence a F. Contudo, 100 admite duas fatorações essencialmente distintas em primos de F, a saber,

$$100 = 4 \cdot 25 \quad \text{e} \quad 100 = 10 \cdot 10$$

Logo, não existe fatoração única em primos de F.

11.8 RELAÇÃO DE CONGRUÊNCIA

Seja m um inteiro positivo. Dizemos que *a é congruente a b módulo m* e denotamos isso por

$$a \equiv b \text{ (módulo } m\text{) ou, simplesmente, } a \equiv b \pmod{m}$$

se m divide a diferença $a - b$. O inteiro m é chamado de *módulo*. A negação de $a \equiv b \pmod{m}$ se escreve $a \not\equiv b \pmod{m}$. Por exemplo:

(i) $87 \equiv 23 \pmod{4}$, pois 4 divide $87 - 23 = 64$.
(ii) $67 \equiv 1 \pmod{6}$, pois 6 divide $67 - 1 = 66$.
(iii) $72 \equiv -5 \pmod{7}$, pois 7 divide $72 - (-5) = 77$.
(iv) $27 \not\equiv 8 \pmod{9}$, uma vez que 9 não divide $27 - 8 = 19$.

Nosso primeiro teorema (demonstrado no Problema 11.34) estabelece que congruência módulo m é uma relação de equivalência.

Teorema 11.21: Seja m um inteiro positivo. Portanto:

(i) Para qualquer inteiro a, temos $a \equiv a \pmod{m}$.
(ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.
(iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Observação: Suponha que m é positivo e a é qualquer inteiro. Pelo Algoritmo da Divisão, existem inteiros q e r com $0 = r \leq m$ tais que $a = mq + r$. Logo

$$mq = a - r \quad \text{ou} \quad m \mid (a - r) \quad \text{ou} \quad a \equiv r \pmod{m}$$

Consequentemente:

(1) Qualquer inteiro a é congruente módulo m a um único inteiro no conjunto

$$\{0, 1, 2, \ldots, m-1\}$$

A unicidade deriva do fato de que m não pode dividir a diferença de dois inteiros como esses

(2) Quaisquer dois inteiros a e b são congruentes módulo m se, e somente se, eles têm o mesmo resto quando divididos por m.

Classes de resíduos

Uma vez que congruência módulo m é uma relação de equivalência, ela particiona o conjunto $\mathbf{Z}$ dos inteiros em classes de equivalência disjuntas chamadas de *classes de resíduos módulo m*. De acordo com tais observações, uma classe de resíduos consiste em todos aqueles inteiros com o mesmo resto, quando divididos por m. Portanto, existem m resíduos como esses e cada classe de resíduos contém exatamente um dos inteiros do conjunto de possíveis restos, ou seja,

$$\{0, 1, 2, \ldots, m-1\}$$

Em termos gerais, um conjunto de m inteiros $\{a_1, a_2, \ldots, a_m\}$ é dito um *sistema completo de resíduos módulo m* se cada a_i se origina de uma classe diferente de resíduos. (Em tal caso, cada a_i é dito um *representante* de sua classe de equivalência.)

Assim, os inteiros de 0 a $m-1$ formam um sistema completo de resíduos. De fato, quaisquer m inteiros consecutivos formam um sistema completo de resíduos módulo m

A notação $[x]_m$, ou simplesmente $[x]$, é empregada para denotar a classe de resíduos (módulo m) contendo um inteiro x, isto é, os inteiros que são congruentes a x. Em outras palavras,

$$[x] = \{a \in \mathbf{Z} \mid a \equiv x \pmod{m}\}$$

Consequentemente, as classes de resíduos podem ser denotadas por

$$[0], [1], [2], \ldots, [m-1]$$

ou simplesmente usando qualquer outra escolha de inteiros em um sistema completo de resíduos.

Exemplo 11.11 As classes de resíduos módulo $m = 6$ são as que se seguem:

$$\begin{aligned}
&[0] = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\}, \quad &[3] = \{\ldots, -15, -9, -3, 3, 9, 15, 21, \ldots\}\\
&[1] = \{\ldots, -17, -11, -5, 1, 7, 13, 19, \ldots\}, \quad &[4] = \{\ldots, -14, -8, -2, 4, 10, 16, 22, \ldots\}\\
&[2] = \{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\}, \quad &[5] = \{\ldots, -13, -7, -1, 5, 11, 17, 23, \ldots\}
\end{aligned}$$

Note que $\{-2, -1, 0, 1, 2, 3\}$ também é um sistema completo de resíduos módulo $m = 6$, e esses representantes têm valores absolutos mínimos.

Aritmética da congruência

O próximo teorema (demonstrado no Problema 11.35) nos diz que, sob adição e multiplicação, a relação de congruência se comporta de maneira muito semelhante à igualdade. Ou seja:

Teorema 11.22: Suponha que $a \equiv c \pmod{m}$ e $b \equiv d \pmod{m}$. Então:

(i) $a + b \equiv c + d \pmod{m}$; (ii) $a \cdot b \equiv c \cdot d \pmod{m}$

Observação: Suponha que $p(x)$ é um polinômio com coeficientes inteiros. Se $s \equiv t \pmod{m}$, então, usando o Teorema 11.22 repetidamente, podemos mostrar que $p(s) \equiv p(t) \pmod{m}$.

Exemplo 11.12 Observe que $2 \equiv 8 \pmod 6$ e $5 \equiv 41 \pmod 6$. Então:

(a) $2 + 5 \equiv 8 + 41 \pmod 6$ ou $7 \equiv 49 \pmod 6$

(b) $2 \cdot 5 \equiv 8 \cdot 41 \pmod 6$ ou $10 \equiv 328 \pmod 6$

(c) Suponha que $p(x) = 3x^2 - 7x + 5$. Logo,

$$p(2) = 12 - 14 + 5 = 3 \text{ e } p(8) = 192 - 56 + 5 = 141$$

Portanto, $3 \equiv 141 \pmod 6$.

Aritmética de classes de resíduos

Adição e multiplicação são definidas para nossas classes de resíduos módulo m como se segue:

$$[a] + [b] = [a + b] \text{ e } [a] \cdot [b] = [ab]$$

Por exemplo, considere as classes de resíduos módulo $m = 6$, ou seja,

$$[0], [1], [2], [3], [4], [5]$$

Então

$$[2] + [3] = [5], [4] + [5] = [9] = [3], [2]\cdot[2] = [4], [2]\cdot[5] = [10] = [4]$$

O Teorema 11.22 nos diz que as definições acima são bem estabelecidas, isto é, a soma e o produto de classes de resíduos não depende da escolha de representante da classe de resíduos.

Existe apenas uma quantidade finita m de classes de resíduos módulo m. Logo, podemos facilmente escrever de forma explícita suas tabelas de adição e multiplicação, quando m é pequeno. A Fig. 11-4 mostra as tábuas de adição e multiplicação para as classes de resíduos módulo $m = 6$. Por conveniência notacional, omitimos os colchetes e simplesmente denotamos as classes de resíduos pelos números 0, 1, 2, 3, 4 e 5.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Figura 11-4

Inteiros módulo m, $\mathbf{Z}_m$

O conjunto dos *inteiros módulo m*, denotado por $\mathbf{Z}_m$, refere-se à classe

$$\mathbf{Z}_m = \{0, 1, 2, 3, \ldots, m - 1\}$$

onde adição e multiplicação são definidas pela aritmética módulo m ou, em outras palavras, pelas operações correspondentes para as classes de resíduos. Por exemplo, a Fig. 11-4 pode também ser percebida como as tabuadas de adição e multiplicação para $\mathbf{Z}_6$. Isso significa que:

> Não existe diferença essencial entre $\mathbf{Z}_m$ e a aritmética das classes de resíduos módulo m e, portanto, ambos são empregados.

Leis de cancelamento para congruências

Lembre que inteiros satisfazem a seguinte propriedade:

Lei de Cancelamento: Se $ab = ac$ e $a \neq 0$, então $b = c$

A diferença crítica entre aritmética usual e aritmética módulo m é que a Lei de Cancelamento acima não é verdadeira para congruências. Por exemplo,

$$3 \cdot 1 \equiv 3 \cdot 5 \pmod 6, \quad \text{mas} \quad 1 \not\equiv 5 \pmod 6$$

Ou seja, não podemos cancelar o 3, apesar de $3 \not\equiv 0 \pmod 6$. Contudo, temos a seguinte *Lei Modificada de Cancelamento* para nossas relações de congruência.

Teorema 11.23 (Lei Modificada de Cancelamento): Suponha que $ab \equiv ac \pmod m$ e $\text{mdc}(a, m) = 1$

$$\text{Então, } b \equiv c \pmod m.$$

O teorema acima é uma consequência do seguinte resultado mais geral (provado no Problema 11.37).

Teorema 11.24: Suponha que $ab \equiv ac \pmod m$ e que $d = \text{mdc}(a, m)$. Então, $b \equiv c \pmod{m/d}$.

Exemplo 11.13 Considere a congruência a seguir:

$$6 \equiv 36 \pmod{10} \tag{11.1}$$

Como $\text{mdc}(3, 10) = 1$, mas $\text{mdc}(6, 10) \neq 1$, podemos dividir ambos os lados de (11.1) por 3, mas não por 6. Ou seja,

$$2 \equiv 12 \pmod{10}, \quad \text{mas} \quad 1 \not\equiv 6 \pmod{10}$$

No entanto, pelo Teorema 11.24, podemos dividir ambos os lados de (11.1) por 6 se também dividirmos os módulos por 2, que é igual a $\text{mdc}(6, 10)$. Isto é,

$$1 \equiv 6 \pmod 5$$

Observação: Suponha que p é primo. Então os inteiros de 1 a $p - 1$ são primos de p. Assim, a lei de cancelamento usual vale quando o módulo é um primo p. Ou seja:

Se $ab \equiv ac \pmod p$ e $a \not\equiv 0 \pmod p$, então $b \equiv c \pmod p$.

Portanto, $\mathbf{Z_p}$, o conjunto dos inteiros módulo um primo p, tem um papel muito especial em teoria dos números.

Sistemas reduzidos de resíduos, função phi de Euler

A Lei Modificada de Cancelamento, Teorema 11.23, é indicativa do papel especial executado por aqueles inteiros que são primos do módulo m (coprimos). Notamos que a é um coprimo de m se, e somente se, todo elemento da classe de resíduos $[a]$ é coprimo de m. Assim, podemos falar de uma classe de resíduos que é coprima de m.

O número de classes de resíduos coprimas de m ou, equivalentemente, o número de inteiros entre 1 e m (inclusive) que são coprimos de m é denotado por

$$\phi\,(m)$$

A função $\phi\,(m)$ é chamada de *função phi de Euler*. A lista de números entre 1 e m que são coprimos de m ou, em termos mais gerais, qualquer lista de $\phi\,(m)$ inteiros incongruentes que são coprimos de m é chamada de *sistema reduzido de resíduos módulo m*.

Exemplo 11.14

(a) Considere o módulo $m = 15$. Há oito inteiros entre 1 e 15 que são coprimos de 15:

$$1, 2, 4, 7, 8, 11, 13, 14$$

Logo, $\phi(15) = 8$, e os oito inteiros acima formam um sistema reduzido de resíduos módulo 15.

(b) Considere qualquer primo p. Todos os números $1, 2, \ldots, p-1$ são coprimos de p; logo, $\phi(p) = p - 1$.

Uma função f com domínio nos inteiros positivos N é chamada de *multiplicativa* se, quando a e b são primos entre si,

$$f(ab) = f(a)f(b)$$

O teorema a seguir (demonstrado no Problema 11.44) se aplica.

Teorema 11.25: A função phi de Euler é multiplicativa. Ou seja, se a e b são primos entre si, então

$$\phi(ab) = \phi(a)\,\phi(b)$$

11.9 EQUAÇÕES DE CONGRUÊNCIA

Uma *equação de congruência polinomial* ou, simplesmente, uma *equação de congruência* (relativamente a uma incógnita x) é uma equação da forma

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m} \tag{11.2}$$

Tal equação é dita de *grau n* se $a \not\equiv 0 \pmod{m}$.

Suponha que $s \equiv t \pmod{m}$. Então s é uma solução de (11.2) se, e somente se, t é uma solução de (11.2). Assim, o *número de soluções* de (11.2) é definido como o número de soluções incongruentes ou, equivalentemente, o número de soluções no conjunto

$$\{0, 1, 2, \ldots, m-1\}$$

É claro que essas soluções sempre podem ser encontradas por teste, ou seja, substituindo cada um dos m números em (11.2) para verificar se eles, de fato, satisfazem a equação.

O *conjunto completo de soluções* de (11.2) é um conjunto máximo de soluções incongruentes quando a *solução geral* de (11.2) é o conjunto de todas as soluções inteiras de (11.2). A solução geral de (11.2) pode ser determinada, adicionando todos os múltiplos do módulo m a qualquer conjunto completo de soluções.

Exemplo 11.15 Considere as equações.

(a) $x^2 + x + 1 \equiv 0 \pmod{4}$, (b) $x^2 + 3 \equiv 0 \pmod{6}$, (c) $x^2 - 1 \equiv 0 \pmod{8}$

Aqui encontramos as soluções por teste.

(a) Não há soluções, uma vez que 0, 1, 2 e 3 não satisfazem a equação.

(b) Existe apenas uma solução entre $0, 1, \ldots, 5$, que é 3. Logo, a solução geral consiste nos inteiros $3 + 6k$, onde $k \in \mathbf{Z}$.

(c) Há quatro soluções, 1, 3, 5 e 7. Isso mostra que uma equação de congruência de grau n pode ter mais de n soluções.

Enfatizamos que não estamos apenas interessados em estudar equações de congruência para encontrar suas soluções, isso sempre pode ser conseguido por inspeção. Estamos prioritariamente interessados em desenvolver técnicas que nos ajudem a encontrar tais soluções, e uma teoria que nos diga as condições sob as quais existam soluções e o número delas. Tal teoria vale para equações de congruência linear que investigamos a seguir. Também discutimos Teorema Chinês do Resto, que é essencialmente um sistema de equações de congruência linear.

Observação 1: Os coeficientes de uma equação de congruência podem sempre ser reduzidos módulo m, pois resultariam em uma equação *equivalente*, ou seja, uma equação com as mesmas soluções. Por exemplo, as equações a seguir são equivalentes, uma vez que os coeficientes são congruentes módulo $m = 6$:

$$15x^2 + 28x + 14 \equiv 0 \pmod 6,\ 3x^2 + 4x + 2 \equiv 0 \pmod 6,\ 3x^2 - 2x + 2 \equiv 0 \pmod 6.$$

Usualmente, escolhemos coeficientes entre 0 e $m - 1$ ou entre $-m/2$ e $m/2$.

Observação 2: Como estamos realmente procurando por soluções de (11.2) entre as classes de resíduos módulo m e não entre os inteiros, podemos ver (11.2) como uma equação sobre os inteiros módulo m, no lugar de uma equação sobre $\mathbf{Z}$, o conjunto dos inteiros. Neste contexto, o número de soluções de (11.2) é simplesmente o número de soluções em $\mathbf{Z}_m$.

Equação de congruência linear: $ax \equiv 1 \pmod m$

Primeiro, consideramos o caso particular da equação de congruência linear

$$ax \equiv 1 \pmod m \tag{11.3}$$

onde $a \not\equiv 0 \pmod m$. A história completa dessa equação é dada no teorema a seguir (demonstrado no Problema 11.57).

Teorema 11.26: Se a e m são primos entre si, então $ax \equiv 1 \pmod m$ admite uma única solução; caso contrário, não tem solução.

Exemplo 11.16

(a) Considere a equação de congruência $6x \equiv 1 \pmod{33}$. Como $\text{mdc}(6, 33) = 3$, essa equação não tem soluções.

(b) Considere a equação de congruência $7x \equiv 1 \pmod 9$. Como $\text{mdc}(7, 9) = 1$, a equação tem uma única solução. Testando os números $0, 1, \ldots, 8$, descobrimos que

$$7(4) = 28 \equiv 1 \pmod 9$$

Portanto, $x = 4$ é nossa única solução. (A solução geral é $4 + 9k$, para $k \in \mathbf{Z}$.)

Suponha que existe uma solução para (11.3), ou seja, que $\text{mdc}(a, m) = 1$. Além disso, suponha que o módulo m é grande. Então, o algoritmo euclidiano pode ser empregado para encontrar uma solução de (11.3). Especificamente, usamos o algoritmo euclidiano para determinar x_0 e y_0 tais que

$$ax_0 + my_0 = 1$$

A partir disso, segue que $ax_0 \equiv 1 \pmod m$, isto é, x_0 é uma solução de (11.3).

Exemplo 11.17 Considere a seguinte equação de congruência:

$$81 \equiv 1 \pmod{256}$$

Por observação ou aplicação do algoritmo euclidiano a 81 e 256, descobrimos que $\text{mdc}(81, 256) = 1$. Portanto, a equação admite uma única solução. Testar pode não ser uma maneira eficiente de encontrar essa solução, uma vez que o módulo $m = 256$ é relativamente grande. Logo, aplicamos o algoritmo euclidiano em $a = 81$ e $m = 256$. Especificamente, como no Exemplo 11.6, descobrimos $x_0 = -25$ e $y_0 = 7$ tais que

$$81x_0 + 256y_0 = 1$$

Isso significa que $x_0 = -25$ é uma solução da equação de congruência dada. Adicionando $m = 256$ a -25, obtemos a seguinte solução única entre 0 e 256:

$$x = 231$$

Equação de congruência linear: $ax \equiv b \pmod{m}$

Agora consideramos a equação de congruência linear mais geral

$$ax \equiv b \pmod{m} \tag{11.4}$$

onde $a \not\equiv 0 \pmod{m}$. Primeiro, levamos em conta o caso (provado no Problema 11.58) onde a e m são coprimos.

Teorema 11.27: Suponha que a e m são primos entre si. Então $ax \equiv b \pmod{m}$ tem uma única solução. Além disso, se s é a solução única para $ax \equiv 1 \pmod{m}$, então a solução única para $ax \equiv b \pmod{m}$ é $x = bs$.

Exemplo 11.18

(a) Considere a equação de congruência $3x \equiv 5 \pmod{8}$. Como 3 e 8 são coprimos, a equação tem uma única solução. Testando os inteiros $0, 1, \dots, 7$, descobrimos que

$$3(7) = 21 \equiv 5 \pmod{8}$$

Logo, $x = 7$ é a solução única da equação.

(b) Considere a equação de congruência linear

$$33x \equiv 38 \pmod{280} \tag{11.5}$$

Uma vez que $\text{mdc}(33, 280) = 1$, a equação admite uma única solução. Testar pode não ser uma maneira eficiente de descobrir essa solução, pois o módulo $m = 280$ é relativamente grande. Aplicamos o algoritmo euclidiano para determinar primeiro uma solução de

$$33x \equiv 1 \pmod{280} \tag{11.6}$$

Ou seja, como no Exemplo 11.6, sabemos que $x_0 = 17$ e $y_0 = 2$ é uma solução de

$$33x_0 + 280y_0 = 1$$

Isso significa que $s = 17$ é uma solução para (11.6). Então

$$sb = 17(38) = 646$$

é uma solução de (11.5). Dividindo 646 por $m = 280$, obtemos o resto

$$x = 86$$

que é a única solução de (11.5) entre 0 e 280. (A solução geral é $86 + 280k$, com $k \in \mathbf{Z}$.)

A história completa do caso geral de (11.4) está encerrada no seguinte teorema (provado no Problema 11.59).

Teorema 11.28: Considere a equação $ax \equiv b \pmod{m}$, onde $d = \text{mdc}(a, m)$.

(i) Suponha que d não divide b. Então $ax \equiv b \pmod{m}$ não tem solução.

(ii) Suponha que d divide b. Então $ax \equiv b \pmod{m}$ tem d soluções, as quais são todas congruentes módulo M à solução única de

$$Ax \equiv B \pmod{M}, \text{ onde } A = a/d,\ B = b/d,\ M = m/d.$$

Enfatizamos que o Teorema 11.27 se aplica à equação $Ax \equiv B \pmod{M}$ do Teorema 11.28, pois $\text{mdc}(A, M) = 1$.

Exemplo 11.19 Resolva cada equação de congruência: (a) $4x \equiv 9 \pmod{14}$; (b) $8x \equiv 12 \pmod{28}$.

(a) Note que $\text{mdc}(4, 14) = 2$. Contudo, 2 não divide 9. Logo, a equação não admite solução.

(b) Observe que $d = \text{mdc}(8, 28) = 4$ e que $d = 4$ divide 12. Assim, a equação tem $d = 4$ soluções. Dividindo cada termo na equação por $d = 4$, obtemos a equação de congruência (11.7) que tem uma única solução.

$$2x \equiv 3 \pmod 7 \tag{11.7}$$

Testando os inteiros 0, 1, . . . , 6, descobrimos que 5 é a solução única de (11.7). Agora adicionamos $d - 1 = 3$ múltiplos de 7 à solução 5 de (11.7), obtendo:

$$5 + 7 = 12, \quad 5 + 2(7) = 19, \quad 5 + 3(7) = 26.$$

Consequentemente, 5, 12, 19 e 26 são as $d = 4$ soluções exigidas da equação original $8x \equiv 12 \pmod{28}$.

Observação: A solução da equação (11.7) do Exemplo 11.19 foi obtida por inspeção. No entanto, no caso em que m é grande, podemos sempre usar o algoritmo euclidiano para encontrar sua solução única, como no Exemplo 11.17.

Teorema chinês do resto

Há um velho problema chinês que levanta a seguinte questão.

> Existe um inteiro positivo x que dividido por 3 tem resto 2, dividido por 5 tem resto 4 e dividido por 7 tem resto 6?

Em outras palavras, buscamos por uma solução das três equações de congruência a seguir:

$$x \equiv 2 \pmod 3, \; x \equiv 4 \pmod 5, \; x \equiv 6 \pmod 7$$

Observe que os módulos 3, 5 e 7 são primos entre si se tomados dois a dois. Logo, o teorema a seguir (provado no Problema 11.60) se aplica; ele nos diz que existe uma única solução módulo $M = 3 \cdot 5 \cdot 7 = 105$.

Teorema 11.29 (Teorema Chinês do Resto): Considere o sistema

$$x \equiv r_1 \pmod{m_1}, \; x \equiv r_2 \pmod{m_2}, \; \cdots, \; x \equiv r_k \pmod{m_k} \tag{11.8}$$

onde os m_i são primos entre si, tomados dois a dois. Então o sistema tem uma única solução módulo $M = m_1 m_2 \cdots m_k$.

É possível realmente apresentar uma fórmula explícita para a solução do sistema (11.8) no Teorema 11.29, que apresentamos como uma proposição.

Proposição 11.30: Considere o sistema (11.8) de equações de congruência. Sejam $M = m_1 m_2 \ldots m_k$ e

$$M_1 = \frac{M}{m_1}, \quad M_2 = \frac{M}{m_2}, \quad \ldots, \quad M_k = \frac{M}{m_k}$$

(Então cada par M_i e m_i é de coprimos.) Sejam $s_1, s_2, \ldots, s_k$ as soluções, respectivamente, das equações de congruência

$$M_1 x \equiv 1 \pmod{m_1}, \; M_2 x \equiv 1 \pmod{m_2}, \; \ldots, \; M_k x \equiv 1 \pmod{m_k}$$

Então o que se segue é uma solução do sistema (11.8):

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k \tag{11.9}$$

Agora resolvemos o problema original de duas maneiras.

Método 1: Primeiro, aplicamos o Teorema Chinês do Resto (TCR) às duas primeiras equações,

$$(a)\ x \equiv 2 \pmod 3 \text{ e } (b)\ x \equiv 4 \pmod 5$$

TCR nos diz que há uma única solução módulo $M = 3 \cdot 5 = 15$. Adicionando múltiplos do módulo $m = 5$ à solução dada $x = 4$ da segunda equação (b), obtemos as três soluções a seguir de (b), as quais são menores do que 15.

$$4, 9, 14$$

Testando cada uma dessas soluções na equação (a), descobrimos que 14 é a única solução de ambas as equações. Agora aplicamos o mesmo processo às duas equações

$$(c)\ x \equiv 14 \pmod{15} \text{ e } (d)\ x \equiv 6 \pmod 7$$

TCR nos diz que existe uma única solução módulo $M = 15 \cdot 7 = 105$. Adicionando múltiplos do módulo $m = 15$ à solução dada $x = 14$ da primeira equação (c), conseguimos as sete soluções a seguir de (b), as quais são menores do que 105.

$$14, 29, 44, 59, 74, 89, 104$$

Testando cada uma dessas soluções de (c) na segunda equação (d), descobrimos que 104 é a única solução de ambas as equações. Portanto, o menor inteiro positivo que satisfaz as três equações é

$$x = 104$$

Essa é a solução do problema chinês.

Método 2: Usando a notação acima, obtemos

$$M = 3 \cdot 5 \cdot 7 = 105,\ M_1 = 105/3 = 35,\ M_2 = 105/5 = 21,\ M_3 = 105/7 = 15$$

Agora buscamos soluções para as equações

$$35x \equiv 1 \pmod 3),\ 21x \equiv 1 \pmod 5,\ 15x \equiv 1 \pmod 7$$

Reduzindo 35 módulo 3, reduzindo 21 módulo 5, e reduzindo 15 módulo 7, temos o sistema

$$2x \equiv 1 \pmod 3,\ x \equiv 1 \pmod 5,\ x \equiv 1 \pmod 7$$

As soluções dessas três equações são, respectivamente,

$$s_1 = 2,\ s_2 = 1,\ s_3 = 1$$

Agora substituímos na fórmula (11.9), para obter a seguinte solução de nosso sistema original:

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 4 + 15 \cdot 1 \cdot 6 = 314$$

Dividindo essa solução pelo módulo $M = 105$, conseguimos o resto

$$x = 104$$

que é a solução única do problema entre 0 e 105

Observação: As soluções acima $s_1 = 2$, $s_2 = 1$ e $s_3 = 1$ foram obtidas por inspeção. Se os módulos são grandes, sempre podemos utilizar o algoritmo euclidiano para encontrar tais soluções, como no Exemplo 11.17

Problemas Resolvidos

Desigualdades, valor absoluto

11.1 Insira o símbolo correto, $<$, $>$ ou $=$, entre cada par de inteiros:

(a) $4 ____ -7$; (b) $-2 ____ -9$; (c) $(-3)^2 ____ 9$; (d) $-8 ____ 3$

Para cada par de inteiros, digamos a e b, determine suas posições relativas na reta numérica **R**, ou, alternativamente, calcule $b - a$ e escreva $a < b$, $a > b$ ou $a = b$ se $b - a$ for positivo, negativo ou zero. Portanto:

(a) $4 > -7$; (b) $-2 > -9$; (c) $(-3)^2 = 9$; (d) $-8 < 3$

11.2 Calcule: (a) $|2 - 5|$, $|-2 + 5|$, $|-2 - 5|$; (b) $|5 - 8| + |2 - 4|$, $|4 - 3| - |3 - 9|$.

Calcule primeiro dentro do valor absoluto:

(a) $|2 - 5| = |-3| = 3$, $|-2 + 5| = |3| = 3$, $|-2 - 5| = |-7| = 7$

(b) $|5 - 8| + |2 - 4| = |-3| + |-2| = 3 + 2 = 5$, $|4 - 3| - |3 - 9| = |1| - |-6| = 1 - 6 = -5$

11.3 Determine a distância d entre cada par de inteiros.

(a) 3 e -7; (b) -4 e 2, (c) 1 e 9; (d) -8 e -3; (e) -5 e -8.

A distância d entre a e b é dada por $d = |a - b| = |b - a|$. Alternativamente, como indicado pela Fig. 11-5, $d = |a| + |b|$ quando a e b têm sinais diferentes, e $d = |a| - |b|$ quando a e b têm o mesmo sinal e $|a| > |b|$. Logo: (a) $d = 3 + 7 = 10$; (b) $d = 4 + 2 = 6$; (c) $d = 9 - 1 = 8$, (d) $d = 8 - 3 = 5$, (e) $d = 8 - 5 = 3$.

(i) $d = |a| + |b|$ (ii) $d = |a| - |b|$

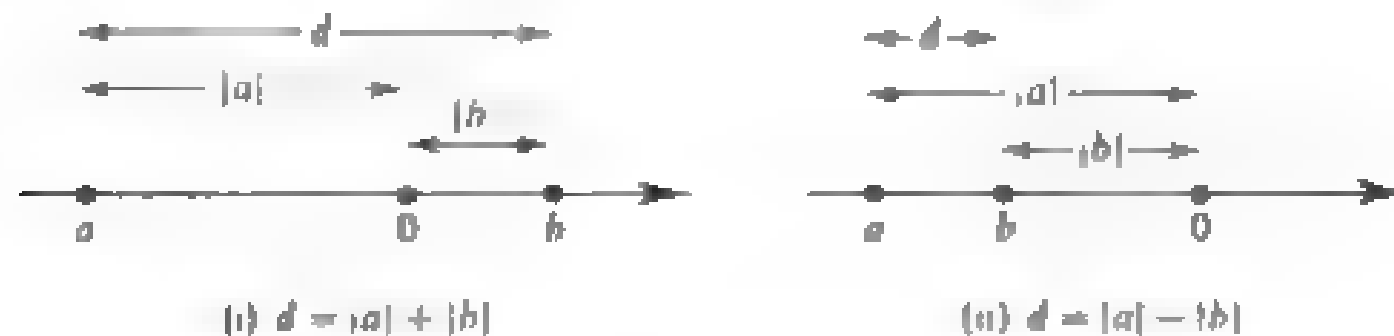



Figura 11-5

11.4 Encontre todos os inteiros n tais que: (a) $1 < 2n - 6 < 14$; (b) $2 < 8 - 3n < 18$.

(a) Adicione 6 aos "três lados" para obter $7 < 2n < 20$. Em seguida, divida todos os lados por 2 (ou multiplique por 1/2) para conseguir $3{,}5 < n < 10$. Logo, $n = 4, 5, 6, 7, 8, 9$.

(b) Adicione -8 aos três lados para obter $-6 < -3n < 10$. Divida por -3 (ou multiplique por $-1/3$) e, uma vez que -3 é negativo, mude o sentido da desigualdade para resultar em

$$2 > n > -3{,}3 \text{ ou } -3{,}3 < n < 2$$

Portanto, $n = -3, -2, -1, 0, 1$

11.5 Prove a Proposição 11.3: Suponha que $a < b$ e que c é um inteiro. Então: (i) $a + c \leq b + c$; (ii) $ac = bc$, quando $c > 0$; mas $ac = bc$, quando $c < 0$.

A proposição é certamente verdadeira quando $a = b$. Logo, precisamos considerar apenas o caso quando $a < b$, isto é, quando $b - a$ é positivo.

(i) A diferença a seguir é positiva: $(b + c) - (a + c) = b - a$. Portanto, $a + c < b + c$.

(ii) Suponha que c é positivo. Pela propriedade $[P_1]$ dos inteiros positivos **N**, o produto $c(b - a)$ é também positivo. Assim, $ac < bc$.

Agora suponha que c é negativo. Então $-c$ é positivo, e o produto $(-c)(b - a) = ac - bc$ também é positivo. Consequentemente, $bc < ac$, quando $ac > bc$.

11.6 Demonstre a Proposição 11.4 (iii): $|ab| = |a||b|$

A prova consiste na análise dos cinco casos a seguir: (*a*) $a = 0$ ou $b = 0$; (*b*) $a > 0$ e $b > 0$; (*c*) $a > 0$ e $b < 0$; (*d*) $ba < 0$ e $b > 0$; (*e*) $ba < 0$ e $b < 0$. Demonstramos apenas o terceiro caso aqui. (*c*) Como $a > 0$ e $b < 0$, $|a| = a$ e $|b| = -b$. Além disso, $ab < 0$. Então, $|ab| = -(ab) = a(-b) = |a||b|$.

11.7 Prove a Proposição 11.4 (iv): $|a \pm b| \leq |a| + |b|$

Agora $ab \leq |ab| = |a||b|$ e, assim, $2ab \leq 2|a||b|$. Logo,

$$(a+b)^2 = a^2 + 2ab + b^2 \leq |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2$$

Mas $\sqrt{(a+b)^2} = |a+b|$. Assim, a raiz quadrada dos termos acima nos leva a $|a+b| \leq |a| + |b|$. Além disso,

$$|a-b| = |a+(-b)| \leq |a| + |-b| = |a| + |b|$$

Indução matemática, princípio da boa ordem

11.8 Prove a proposição de que a soma dos n primeiros inteiros positivos é $n(n+1)/2$, ou seja:

$$P(n): \quad 1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$$

$P(1)$ é verdadeira, pois $1 = \frac{1}{2}(1)(1+1)$. Assumindo que $P(k)$ é verdadeira, adicionamos $k+1$ a ambos os lados de $P(k)$, obtendo

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k+1) &= \frac{1}{2}k(k+1) + (k+1) = \frac{1}{2}[k(k+1) + 2(k+1)] \\ &= \frac{1}{2}[(k+1)(k+2)] \end{aligned}$$

Isso é $P(k+1)$. Consequentemente, $P(k+1)$ é verdadeira, quando $P(k)$ é verdadeira. Pelo Princípio de Indução Matemática, P é verdadeira para todo $n \in \mathbf{N}$.

11.9 Suponha que $a \neq 1$. Mostre que P é verdadeira para todo $n \geq 1$, onde P é definida como se segue:

$$P(n): \quad 1 + a + a^2 + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}$$

$P(1)$ é verdadeira, uma vez que

$$1 + a = \frac{a^2 - 1}{a - 1}$$

Assumindo que $P(k)$ é verdadeira, adicionamos a^{k+1} a ambos os lados de $P(k)$, obtendo

$$\begin{aligned} 1 + a + a^2 + \ldots + a^k + a^{k+1} &= \frac{a^{k+1} - 1}{a - 1} + a^{k+1} = \frac{a^{k+1} - 1 + (a-1)a^{k+1}}{a - 1} \\ &= \frac{a^{k+2} - 1}{a - 1} \end{aligned}$$

Isso é $P(k+1)$. Logo, $P(k+1)$ é verdadeira, quando $P(k)$ é verdadeira. Pelo Princípio de Indução Matemática, P é verdadeira para todo $n \in \mathbf{N}$.

11.10 Suponha que n é um inteiro positivo. Prove que $n \geq 1$. (Isso não é verdadeiro para os números racionais $\mathbf{Q}$.) Em outras palavras, se $P(n)$ é a afirmação de que $n \geq 1$, então $P(n)$ é verdadeira para todo $n \in \mathbf{N}$.

$P(n)$ vale para $n = 1$, uma vez que $1 \geq 1$. Assumindo que $P(k)$ é verdadeira, ou seja, que $k \geq 1$, adicione 1 a ambos os lados para obter

$$k + 1 \geq 1 + 1 = 2 \geq 1$$

Isso é $P(k+1)$. Portanto, $P(k+1)$ é verdadeira, quando $P(k)$ é verdadeira. Pelo Princípio de Indução Matemática, P é verdadeira para todo $n \in \mathbf{N}$

11.11 Suponha que a e b são inteiros positivos. Prove que:

(*a*) Se $b \neq 1$, então $a < ab$.

(*b*) Se $ab = 1$, então $a = 1$ e $b = 1$.

(*c*) Se n é composto, então $n = ab$, onde $1 < a, b < n$.

(*a*) Pelo Problema 11.10, $b > 1$. Portanto, $b - 1 > 0$, isto é, $b - 1$ é positivo. Pela propriedade $[P_1]$ dos inteiros positivos $\mathbf{N}$, o produto a seguir também é positivo:

$$a(b - 1) = ab - a$$

Logo, $a < ab$, como pedido.

(*b*) Suponha que $b \neq 1$. Por (*a*), $a < ab = 1$. Isso contradiz o Problema 11.10; portanto, $b = 1$. Segue então que $a = 1$.

(*c*) Se n não é primo, então n tem um divisor positivo a tal que $a \neq 1$ e $a \neq n$. Então, $n = ab$, onde $b \neq 1$ e $b \neq n$. Assim, pelo Problema 11.10 e pelo item (a), $1 < a, b < ab = n$.

11.12 Demonstre o Teorema 11.6 (Princípio da Boa Ordem): Seja S um conjunto não vazio de inteiros positivos. Então S contém pelo menos um elemento.

Suponha que S não admite menor elemento. Faça M consistindo nos inteiros positivos que são menores do que todo elemento de S. Então, $1 \in M$; caso contrário, $1 \in S$ e 1 seria um menor elemento de S. Seja $k \in M$. Então, k é menor do que todo elemento de S. Portanto, $k + 1 \in M$, caso contrário, $k + 1$ seria um menor elemento de S.

Pelo Princípio de Indução Matemática, M contém todos os inteiros positivos. Portanto, S é vazio, o que contradiz a hipótese de que S é não vazio. Consequentemente, a hipótese original de que S não tem menor elemento não pode ser verdadeira. Desse modo, o teorema é verdadeiro.

11.13 Prove o Teorema 11.5 (indução: segunda forma). Seja P uma proposição definida sobre os inteiros $n \geq 1$, tal que: (i) $P(1)$ é verdadeira; (ii) $P(k)$ é verdadeira quando $P(j)$ é verdadeira para todo $1 < j < k$.

Então P é verdadeira para todo $n \geq 1$.

Seja A o conjunto dos inteiros $n \geq 1$ para os quais P não é verdadeira. Suponha que A seja não vazio. Pelo Princípio da Boa Ordem, A contém um elemento mínimo a_0. De acordo com (i), $a_0 \neq 1$.

Como a_0 é o menor elemento de A, P é verdadeira para todo inteiro j, onde $1 \leq j < a_0$. Por (ii), P é verdadeira para a_0. Isso contradiz o fato de que $a_0 \in A$. Logo, A é vazio e, assim, P é verdadeira para todo inteiro $n > 1$.

Algoritmo da divisão

11.14 Para cada par de inteiros a e b, encontre inteiros q e r tais que $a = bq + r$ e $0 < r < |b|$:

(*a*) $a = 258$ e $b = 12$; (b) $a = 573$ e $b = -16$.

(*a*) Aqui a e b são positivos. Simplesmente divida a por b, ou seja, 258 por 12, digamos, pela divisão longa, para obter o quociente $q = 21$ e o resto $r = 6$. Alternativamente, usando uma calculadora, temos

$$258/12 = 21{,}5,\ q = INT(a/b) = 21,\ r = a - bq = 258 - 12(21) = 6$$

(*b*) Aqui a é positivo, mas b é negativo. Divida a por $|b|$, ou seja, 573 por 16, digamos, com uma calculadora, para obter:

$$a/|b| = 573/16 = 35{,}8125,\ q' = INT(a/|b|) = 35,\ r' = 573 - 16(35) = 13$$

Então

$$573 = (16)(35) + 13 \text{ e } 573 = (-16)(-35) + 13$$

Assim, $q = -35$ e $r = 13$.

11.15 Para cada par de inteiros a e b, encontre inteiros q e r tais que $a = bq + r$ e $0 \leq r < |b|$.

(a) $a = -381$ e $b = 14$; (b) $a = -433$ e $b = -17$.

Aqui a é negativo em cada caso. Portanto, temos que fazer alguns ajustes para garantir que $0 \leq r < |b|$.

(a) Divida $|a| = 381$ por $b = 14$, digamos, com uma calculadora, para obter o quociente $q' = 27$ e o resto $r' = 3$. Então

$$381 = (14)(27) + 3 \text{ e, assim, } -381 = (14)(-27) - 3$$

Mas -3 é negativo e não pode ser o resto r; logo, adicionamos e subtraímos $b = 14$ como se segue:

$$-381 = (14)(-27) - 14 + 14 - 3 = (14)(-28) + 11$$

Dessa forma, $q = -28$ e $r = 11$.

(b) Divida $|a| = 433$ por $|b| = 17$, digamos, com uma calculadora, para obter o quociente $q' = 25$ e o resto $r' = 8$. Então

$$433 = (17)(25) + 8 \quad \text{e, assim,} \quad -433 = (-17)(25) - 8$$

Mas -8 é negativo e não pode ser o resto r; corrigimos isso, adicionando e subtraindo $|b| = 17$ como se segue:

$$-433 = (-17)(25) - 17 + 17 - 8 = (-17)(26) + 9$$

Assim, $q = 26$ e $r = 9$.

11.16 Prove que $\sqrt{2}$ não é racional, isto é, $\sqrt{2} \neq a/b$, onde a e b são inteiros.

Suponha que $\sqrt{2}$ é racional e que $\sqrt{2} = a/b$, onde a e b são inteiros reduzidos aos menores termos, ou seja, mdc$(a, b) = 1$. Elevando ambos os lados ao quadrado, temos

$$2 = \frac{a^2}{b^2} \quad \text{ou} \quad a^2 = 2b^2$$

Então 2 divide a^2. Como 2 é um primo, ele também divide a. Digamos que $a = 2c$. Então

$$2b^2 = a^2 = 4c^2 \quad \text{ou} \quad b^2 = 2c^2$$

Logo, 2 divide b^2. Uma vez que 2 é primo, ele também divide b. Assim, 2 divide ambos a e b. Isso contradiz a hipótese de que mdc$(a, b) = 1$. Portanto, $\sqrt{2}$ não é racional.

11.17 Demonstre o Teorema 11.8 (algoritmo da divisão) para o caso de inteiros positivos. Ou seja, assumindo que a e b são inteiros positivos, prove que existem inteiros não negativos q e r tais que

$$a = bq + r \qquad \text{e} \qquad 0 \leq r < b \tag{11.10}$$

Se $a < b$, escolha $q = 0$ e $r = a$. Se $a = b$, escolha $q = 1$ e $r = 0$. Em qualquer caso, q e r satisfazem (11.10).

A prova agora é por indução em a. Se $a = 1$, então $a < b$ ou $a = b$; logo, o teorema vale quando $a = 1$. Suponha que $a > b$. Então, $a - b$ é positivo e $a - b < a$. Por indução, o teorema vale para $a - b$. Dessa forma, existem q' e r' tais que

$$a - b = bq' + r' \qquad \text{e} \qquad 0 \leq r' < b$$

Logo,

$$a = bq' + b + r' = b(q' + 1) + r'$$

Escolha $q = q' + 1$ e $r = r'$. Então, q e r são inteiros não negativos e satisfazem (11.10). Portanto, o teorema está provado.

11.18 Demonstre o Teorema 11.8 (algoritmo da divisão): Sejam a e b inteiros com $b \neq 0$. Então, existem inteiros q e r tais que $a = bq + r$ e $0 \leq r' < |b|$. Além disso, os inteiros q e r são únicos.

Seja M o conjunto de inteiros não negativos da forma $a - xb$ para algum inteiro x. Se $x = -|a|b$, então $a - xb$ é não negativo; logo, M é não vazio. De acordo com o Princípio da Boa Ordem, M tem elemento mínimo, digamos, r. Como $r \in M$, temos

$$r \geq 0 \qquad \text{e} \qquad r = a - qb$$

para algum inteiro q. Precisamos apenas mostrar que $r < |b|$. Suponha que $r \geq |b|$. Fazendo $r' = r - |b|$, temos $r' \geq 0$ e também $r' < r$, pois $b \neq 0$. Além disso,

$$r' = r - |b| = a - qb - |b| = \begin{cases} a - (q+1)b, & \text{se } b < 0 \\ a - (q-1)b, & \text{se } b > 0 \end{cases}$$

Em qualquer caso, r' pertence a M. Isso contradiz o fato de que r é o menor elemento de M. Consequentemente, $r < |b|$. Assim, a existência de q e r está provada.

Agora mostramos que q e r são únicos. Suponha que existem inteiros q e r e q' e r' tais que

$$a = bq + r \quad \text{e} \quad a = bq' + r', \quad \text{onde} \quad 0 < r, r' < |b|$$

Então, $bq + r = bq' + r'$; portanto,

$$b(q - q') = r' - r$$

Logo, b divide $r' - r$. Mas $|r' - r| < |b|$, uma vez que $0 < r, r' < |b|$. Consequentemente, $r' - r = 0$. Como $b \neq 0$, isso implica que $q - q' = 0$. Portanto, $r' = r$ e $q' = q$; ou seja, q e r são univocamente determinados por a e b.

Divisibilidade, primos, máximo divisor comum

11.19 Encontre todos os divisores de: (a) 18, (b) $256 = 2^8$, (c) $392 = 2^3 \cdot 7^2$.

(a) Como 18 é relativamente pequeno, simplesmente escrevemos todos os inteiros positivos (≤ 18) que dividem 18. Eles são

$$1, \quad 2, \quad 3, \quad 6, \quad 9, \quad 18$$

(b) Como 2 é primo, os divisores positivos de $256 = 2^8$ são simplesmente as potências inferiores de 2, isto é,

$$2^0, \quad 2^1, \quad 2^2, \quad 2^3, \quad 2^4, \quad 2^5, \quad 2^6, \quad 2^7, \quad 2^8$$

Em outras palavras, os divisores positivos de 256 são:

$$1, \quad 2, \quad 4, \quad 8, \quad 16, \quad 32, \quad 64, \quad 128, \quad 256$$

(c) Como 2 e 7 são primos, os divisores positivos de $392 = 2^3 \cdot 7^2$ são produtos de potências inferiores de 2 multiplicadas por potências inferiores de 7, ou seja,

$$2^0 \cdot 7^0, \quad 2^1 \cdot 7^0, \quad 2^2 \cdot 7^0, \quad 2^3 \cdot 7^0, \quad 2^0 \cdot 7, \quad 2^1 \cdot 7, \quad 2^2 \cdot 7, \quad 2^3 \cdot 7^1,$$
$$2^0 \cdot 7^2, \quad 2^1 \cdot 7^2, \quad 2^2 \cdot 7^2, \quad 2^3 \cdot 7^2$$

Em outras palavras, os divisores positivos de 392 são:

$$1, \quad 2, \quad 4, \quad 8, \quad 7, \quad 14, \quad 28, \quad 56, \quad 49, \quad 98, \quad 196, \quad 392$$

(Utilizamos a convenção usual de que $n^0 = 1$ para qualquer número n não nulo.)

11.20 Liste todos os primos entre 50 e 100.

Simplesmente liste todos os números p entre 50 e 100 que não podem ser escritos como o produto de dois inteiros positivos, excluindo 1 e p. Isso nos leva a

$$51, \ 53, \ 57, \ 59, \ 61, \ 67, \ 71, \ 73, \ 79, \ 83, \ 87, \ 89, \ 91, \ 93, \ 97$$

11.21 Sejam $a = 8316$ e $b = 10\,920$.

(a) Encontre $d = \text{mdc}(a, b)$, o máximo divisor comum de a e b.

(b) Determine inteiros m e n tais que $d = ma + nb$.

(c) Encontre mmc(a, b), o mínimo múltiplo comum de a e b.

(a) Aplique o algoritmo euclidiano a a e b. Ou seja, aplique o algoritmo da divisão a a e b e então repetidamente aplique o mesmo procedimento a cada quociente e resto, até obter um resto nulo. Esses passos são ilustrados na Fig. 11-6(a), usando divisão longa, e também na Fig. 11-6(b), onde flechas indicam o quociente e o resto no próximo passo. O último resto diferente de zero é 84. Logo, 84 = mdc(8316, 10920).

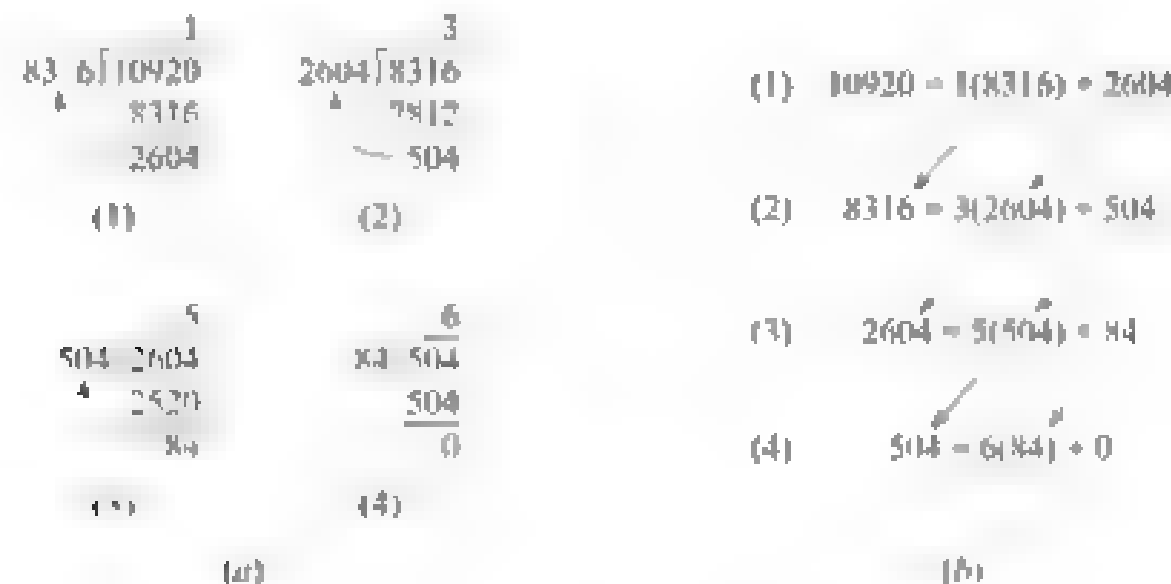



Figura 11-6

(b) Agora encontre m e n tais que $84 = 8316m + 1092n$, "revelando" os passos acima no algoritmo euclidiano. Especificamente, os três primeiros quocientes na Fig. 11-6 nos levam às equações:

$$(1)\ 2604 = 10\,920 - 1(8316); \quad (2)\ 504 = 8316 - 3(2604); \quad (3)\ 84 = 2604 - 5(504)$$

A equação (3) nos diz que $d = 84$ é uma combinação linear de 2604 e 504. Use (2) para substituir 504 em (3), de modo que 84 possa ser escrito como uma combinação linear de 2604 e 8316 como se segue.

$$\begin{aligned}(5)\ 84 &= 2604 - 5[8316 - 3(2604)] = 2604 - 5(8316) + 15(2604)\\ &= 16(2604) - 5(8316)\end{aligned}$$

Essa é a nossa combinação linear desejada. Em outras palavras, $m = -21$ e $n = 16$.

(c) Pelo Teorema 11.16,

$$\text{mmc}(a, b) = \frac{|ab|}{\text{mdc}(a, b)} = \frac{(8316)(10\,920)}{84} = 1\,081\,080$$

11.22 Encontre a fatoração única de cada número: (a) 135, (b) 1330; (c) 3105; (d) 211.

(a) $135 = 5 \cdot 27 = 5 \cdot 3 \cdot 3 \cdot 3$ ou $135 = 3^3 \cdot 5$

(b) $1330 = 2 \cdot 665 = 2 \cdot 5 \cdot 133 = 2 \cdot 5 \cdot 7 \cdot 19$

(c) $3105 = 5 \cdot 621 = 5 \cdot 3 \cdot 207 = 5 \cdot 3 \cdot 3 \cdot 69 = 5 \cdot 3 \cdot 3 \cdot 3 \cdot 23$, ou $3105 = 3^3 \cdot 5 \cdot 23$

(d) Nenhum dos primos 2, 3, 5, 7, 11, 13 divide 211, logo, 211 não pode ser fatorado, ou seja, 211 é um primo.

Observação: Precisamos testar apenas os primos menores do que $\sqrt{211}$.

11.23 Sejam $a = 2^3 \cdot 3^5 \cdot 5^4 \cdot 11^6 \cdot 17^3$ e $b = 2^5 \cdot 5^3 \cdot 7^2 \cdot 11^4 \cdot 13^2$. Encontre mdc($a$, b) e mmc(a, b).

Os primos p_i que aparecem em ambos a e b também ocorrem em mdc(a, b). Além disso, o expoente de p_i em mdc(a, b) é o menor dos expoentes em a e b. Logo,

$$\text{mdc}(a, b) = 2^3 \cdot 5^3 \cdot 11^4$$

Os primos p_i que ocorrem em a ou b também aparecem em mmc(a, b). Além disso, o expoente de p_i em mmc(a, b) é o maior dos expoentes em a e b. Portanto,

$$\text{mmc}(a, b) = 2^5 \cdot 3^5 \cdot 5^4 \cdot 7^2 \cdot 11^6 \cdot 13^7 \cdot 17^3$$

11.24 Prove o Teorema 11.9: Suponha que a, b e c são inteiros.

(i) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

(ii) Se $a \mid b$, então, para qualquer inteiro x, $a \mid bx$.

(iii) Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$ e $a \mid (b - c)$.

(iv) Se $a \mid b$ e $b \neq 0$, então $a = \pm b$ ou $|a| < |b|$.

(v) Se $a \mid b$ e $b \mid a$, então $|a| = |b|$, ou seja, $a = \pm b$.

(vi) Se $a \mid 1$, então $a = \pm 1$.

(i) Se $a \mid b$ e $b \mid c$, então existem inteiros x e y tais que $ax = b$ e $by = c$. Substituindo b por ax, obtemos $axy = c$. Logo, $a \mid c$.

(ii) Se $a \mid b$, então existe um inteiro c tal que $ac = b$. Multiplicando a equação por x, obtemos $acx = bx$. Portanto, $a \mid bx$.

(iii) Se $a \mid b$ e $a \mid c$, então existem inteiros x e y tais que $ax = b$ e $ay = c$. Adicionando as igualdades, obtemos

$$ax + ay = b + c \quad \text{e, assim,} \quad a(x + y) = b + c$$

Logo, $a \mid (b + c)$. Subtraindo as igualdades $ay = b$ e $by = c$, obtemos

$$ax - ay = b - c \quad \text{e, assim,} \quad a(x - y) = b - c.$$

Portanto, $a \mid (b - c)$.

(iv) Se $a \mid b$, então existe c tal que $ac = b$. Logo,

$$|b| = |ac| = |a||c|$$

Desse modo, $|c| = 1$ ou $|a| < |a||c| = |b|$. Se $|c| = 1$, então $c = \pm 1$; onde $a = \pm b$, como exigido.

(v) Se $a \mid b$, então $a = \pm b$ ou $|a| < |b|$. Se $|a| < |b|$, então $b \nmid a$. Logo, $a = \pm b$.

(vi) Se $a \mid 1$ então $a = \pm 1$ ou $|a| < |1| = 1$. Pelo Problema 11.11, $|a| \geq 1$. Portanto, $a = \pm 1$.

11.25 Um conjunto não vazio J de $\mathbf{Z}$ é dito um *ideal* se J tem as duas propriedades a seguir:

(1) Se $a, b \in J$, então $a + b \in J$. (2) Se $a \in J$ e $n \in \mathbf{Z}$, então $na \in J$.

Seja d o menor inteiro positivo em um ideal $J \neq \{0\}$. Prove que d divide todo elemento de J.

Como $J \neq \{0\}$, existe $a \in J$ com $a \neq 0$. Então, $-a = (-1)a \in J$. Logo, J contém elementos positivos. De acordo com o Princípio da Boa Ordem, J contém um menor inteiro positivo e, portanto, d existe. Agora faça $b \in J$. Dividindo b por d, o algoritmo da divisão nos diz que existem q e r tais que

$$b = qd + r \quad \text{e} \quad 0 \leq r < d$$

Isto é, $b, d \in J$ e J é um ideal, logo, $b + (-q)d = r$ também pertence a J. Pela propriedade de elemento mínimo de d, devemos ter $r = 0$. Logo, $d \mid b$, como exigido.

11.26 Demonstre o Teorema 11.13. Seja d o menor inteiro positivo da forma $ax + by$. Então $d = \text{mdc}(a, b)$.

Considere o conjunto $J = \{ax + yb \mid x, y \in \mathbf{Z}\}$. Então

$$a = 1(a) + 0(b) \in J \quad \text{e} \quad b = 0(a) + 1(b) \in J$$

Suponha também que $s, t \in J$, digamos, $s = x_1a + y_1b$ e $t = x_2a + y_2b$. Então, para qualquer $n \in \mathbf{Z}$, os números a seguir pertencem a J:

$$s + t = (x_1 + x_2)a + (y_1 + y_2)b \quad \text{e} \quad ns = (nx_1)a + (ny_1)b$$

Assim, J é um ideal. Seja d o menor elemento positivo de J. Afirmamos que $d = \text{mdc}(a, b)$.

De acordo com o Problema 11.25, d divide todo elemento de J. Portanto, em especial, d divide a e b. Agora suponha que h divide ambos a e b. Então h divide $xa + yb$ para quaisquer x e y, isto é, h divide todo elemento de J. Logo, h divide d e, assim, $h \leq d$. Consequentemente, $d = \text{mdc}(a, b)$.

11.27 Demonstre o Teorema 11.17: Suponha que $\text{mdc}(a, b) = 1$ e que a e b dividem c. Então ab divide c.

Como $\text{mdc}(a, b) = 1$, existem x e y tais que $ax + by = 1$. Uma vez que $a \mid c$ e $b \mid c$, existem m e n tais que $c = ma$ e $c = nb$. Multiplicando $ax + by = 1$ por c, temos

$$acx + bcy = c \quad \text{ou} \quad a(nb)x + b(ma)y = c \quad \text{ou} \quad ab(nx + my) = c$$

Portanto, ab divide c.

11.28 Demonstre o Corolário 11.19: Suponha que um primo p divida um produto ab. Então, $p \mid a$ ou $p \mid b$.

Suponha que p não divide a. Então $\text{mdc}(p, a) = 1$, pois os únicos divisores de p são ± 1 e $\pm p$. Assim, existem inteiros m e n tais que $1 = mp + na$. Multiplicando por b, temos $b = mpb + nab$. Por hipótese, $p \mid ab$, digamos, $ab = cp$. Então:

$$b = mpb + nab = mpb + ncp = p(mb + nc)$$

Logo, $p \mid b$, como pedido.

11.29 Prove: (a) Suponha que $p \mid q$, onde p e q são primos. Então $p = q$.

(b) Suponha que $p \mid q_1 q_2 \cdots q_r$, onde p e cada q_i são primos. Então p é igual a um dos q_i.

(a) Os únicos divisores de q são ± 1 e $\pm q$. Como $p > 1$, $p = q$.

(b) Se $r = 1$, então $p = q_1$, de acordo com (a). Suponha que $r > 1$. Pelo Problema 11.28 (Corolário 11.19), $p \mid q_1$ ou $p \mid (q_2 \cdots q_r)$. Se $p \mid q_1$, então $p = q_1$, por (a). Caso contrário, então $p \mid (q_2 \cdots q_r)$. Repetimos o argumento. Ou seja, temos $p = p_2$ ou $p \mid (q_3 \cdots q_r)$. Finalmente (ou por indução), p deve ser igual a um dos q_i.

11.30 Prove o Teorema Fundamental da Aritmética (Teorema 11.20): Todo inteiro $n > 1$ pode ser expresso univocamente (exceto pela ordem) como um produto de primos.

Já demonstramos o Teorema 11.11 no qual se estabelece que tal produto de primos existe. Logo, precisamos apenas mostrar que esse produto é único (exceto quanto à ordem). Suponha que

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r$$

onde cada p_i e cada q_j são primos. Observe que $p_1 \mid (q_1 q_2 \cdots q_r)$. De acordo com o Problema 11.29, p_1 é igual a um dos q_j. Rearranjamos os q_j, de modo que $p_1 = q_1$. Então

$$p_1 p_2 \cdots pk = p_1 q_2 \cdots q_r \quad \text{e, portanto,} \quad p_2 \cdots p_k = q_2 \cdots q_r$$

Pelo mesmo argumento, podemos rearranjar os demais q_j, de modo que $p_2 = q_2$, e assim por diante. Logo, n pode ser expresso univocamente como um produto de primos (exceto quanto à ordem).

Congruências

11.31 Quais das seguintes expressões são verdadeiras?

(a) $446 \equiv 278 \pmod 7$, (c) $269 \equiv 413 \pmod{12}$, (e) $445 \equiv 536 \pmod{18}$,

(b) $793 \equiv 682 \pmod 9$, (d) $473 \equiv 369 \pmod{26}$, (f) $383 \equiv 126 \pmod{15}$

Lembre que $a \equiv b \pmod m$ se, e somente se, m divide $a - b$.

(a) Encontre a diferença $446 - 278 = 168$. Divida a diferença 168 pelo módulo $m = 7$. O resto é 0; logo, a afirmação é verdadeira.

(b) Divida a diferença $793 - 682 = 111$ pelo módulo $m = 9$. O resto não é 0, portanto, a afirmação é falsa.

(c) Verdadeira; pois 12 divide $269 - 413 = -144$.

(d) Verdadeira; pois 26 divide $473 - 369 = 104$.

(e) Falsa; uma vez que 18 não divide $445 - 536 = -91$.

(f) Falsa; uma vez que 15 não divide $383 - 126 = 157$.

11.32 Encontre o menor número inteiro em valor absoluto que é congruente módulo $m = 7$ a cada um dos seguintes números: (a) 386, (b) 257, (c) -192; (d) -466.

O inteiro deve estar no conjunto $\{-3, -2, -1, 0, 1, 2, 3\}$.

(a) Dividindo 386 por $m = 7$, temos um resto 1; logo, $386 \equiv 1 \pmod 7$.

(b) Dividindo 257 por $m = 7$, temos um resto 5; logo, $257 \equiv 5 \equiv -2 \pmod 7$. (Obtemos -2, subtraindo $m = 7$ de 5.)

(c) Dividindo 192 por m = 7, temos um resto 3; logo, $-192 \equiv -3 \pmod 7$.

(d) Dividindo 466 por $m = 7$, temos um resto 4, portanto, $-466 \equiv -4 \equiv 3 \pmod 7$. (Obtemos 3, adicionando o módulo $m = 7$ a -4.)

11.33 Determine todos os números entre -50 e 50 que são congruentes a 21 módulo $m = 12$, ou seja, encontre todos os x tais que $-50 \le x \le 50$ e $x \equiv 21 \pmod{12}$.

Adicione e subtraia múltiplos do módulo $m = 12$ ao número dado 21 para obter

$$21 + 0 = 21 \qquad 21 + 12 = 33 \qquad 33 + 12 = 46 \qquad 21 - 12 = 9$$
$$9 - 12 = -3 \qquad -3 - 12 = -15 \qquad -15 - 12 = -27 \qquad -27 - 12 = -39$$

Isto é, $-39, -27, -15, -3, 9, 21, 33, 46$.

11.34 Prove o Teorema 11.21: Seja m um inteiro positivo. Então:

(i) Para qualquer inteiro a, temos $a \equiv a \pmod m$.

(ii) Se $a \equiv b \pmod m$, então $b \equiv a \pmod m$.

(iii) Se $a \equiv b \pmod m$ e $b \equiv c \pmod m$, então $a \equiv c \pmod m$.

(i) A diferença $a - a = 0$ é divisível por m; logo, $a \equiv a \pmod m$.

(ii) Se $a \equiv b \pmod m$, então $m \mid (a - b)$. Portanto, m divide $-(a - b) = b - a$. Logo, $b \equiv a \pmod m$.

(iii) Sabemos que $m \mid (a - b)$ e $m \mid (b - c)$. Assim, m divide a soma $(a - b) + (b - c) = a - c$. Então, $a \equiv c \pmod m$.

11.35 Demonstre o Teorema 11.22. Suponha que $a \equiv c \pmod m$ e $b \equiv d \pmod m$. Logo:

(i) $a + b \equiv c + d \pmod m$, (ii) $a \cdot b \equiv c \cdot d \pmod m$.

Sabemos que $m \mid (a - c)$ e $m \mid (b - d)$.

(i) Então m divide a soma $(a - c) + (b - d) = (a + b) - (c + d)$. Logo, $a + b \equiv c + d \pmod m$.

(ii) Então m divide $b(a - c) = ab - bc$ e m divide $c(b - d) = bc - cd$. Assim, m divide a soma $(ab - bc) + (bc - cd) = ab - cd$. Logo, $ab \equiv cd \pmod m$.

11.36 Seja $d = \text{mdc}(a, b)$. Mostre que a/d e b/d são primos entre si.

Existem x e y tais que $d = xa + yb$. Dividindo a equação por d, obtemos $1 = x(a/d) + y(b/d)$. Logo, a/d e b/d são primos entre si.

11.37 Demonstre o Teorema 11.24: Suponha que $ab \equiv ac \pmod m$ e $d = \text{mdc}(a, m)$. Logo, $b \equiv c \pmod{m/d}$.

Por hipótese, m divide $ab - ac = a(b - c)$. Logo, existe um inteiro x tal que $a(b - c) = mx$. Dividindo por d, temos $(a/d)(b - c) = (m/d)x$. Assim, m/d divide $(a/d)(b - c)$. Como m/d e a/d são primos entre si, m/d divide $b - c$. Ou seja, $b \equiv c \pmod{m/d}$, como pedido.

Sistemas de resíduos, função Phi de Euler

11.38 Para cada módulo m, exiba dois sistemas completos de resíduos, um consistindo nos menores inteiros não negativos e o outro consistindo nos inteiros com os menores valores absolutos: (a) $m = 9$; (b) $m = 12$.

No primeiro caso, escolha $\{0, 1, 2, \ldots, m - 1\}$ e, no segundo, caso escolha

$$\{-(m-1)/2, \ldots, -1, 0, 1, \ldots, (m-1)/2\} \quad \text{ou} \quad \{-(m-2)/2, \ldots, -1, 0, 1, \ldots, m/2\}$$

dependendo se m é par ou ímpar

(a) $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ e $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

(b) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ e $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$.

11.39 Encontre um sistema reduzido de resíduos módulo m e $\phi(m)$, onde. (a) $m = 9$, (b) $m = 16$, (c) $m = 7$

Escolha os números positivos menores do que m e primos de m. A quantia de tais números é $\phi(m)$.

(a) $\{1, 2, 4, 5, 7, 8\}$, logo, $\phi(9) = 6$.

(b) $\{1, 3, 5, 7, 9, 11, 13, 15\}$; logo, $\phi(16) = 8$.

(c) $\{1, 2, 3, 4, 5, 6\}$, logo, $\phi(7) = 6$. (Isso é esperado, pois $\phi(p) = p - 1$ para qualquer primo p.)

11.40 Lembre que $Sm = 0, 1, 2, \ldots, m - 1$ é um sistema completo de resíduos módulo m. Prove que.

(a) Quaisquer m inteiros consecutivos é um sistema completo de resíduos módulo m

(b) Se $\text{mdc}(a, m) = 1$, então $aS_m = \{0, a, 2a, 3a, \ldots, (m-1)a\}$ é um sistema completo de resíduos módulo m.

(a) Considere qualquer outra sequência de m inteiros, digamos, $\{a, a+1, a+2, \ldots, a+(m-1)\}$. O valor absoluto da diferença s entre quaisquer dois dos inteiros é menor do que m. Assim, m não divide s e, portanto, os números são incongruentes módulo m.

(b) Suponha que $ax \equiv ay \pmod{m}$, onde $x, y \in S_m$. Uma vez que $\text{mdc}(a, m) = 1$, a Lei Modificada de Cancelamento do Teorema 11.24 nos diz que $x \equiv y \pmod{m}$. Como $x, y \in S_m$, devemos ter $x = y$. Isto é, aS_m é um sistema completo de resíduos módulo m.

11.41 Exiba um sistema compelto de resíduos módulo $m = 8$ consistindo em múltiplos de 3.

De acordo com o Problema 11.40(b), $3S_8 = \{0, 3, 6, 9, 12, 15, 18, 21\}$ é um sistema completo de resíduos módulo $m = 8$.

11.42 Mostre que se p é um primo, então $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Claramente, $\text{mdc}(a, p^n) \neq 1$ se, e somente se, p divide a. Assim, os únicos números entre 1 e p^n que não são primos de p^n são os múltiplos de p, ou seja, $p, 2p, 3p, \ldots, p^{n-1}(p)$. Existem p^{n-1} múltiplos de p. Todos os outros números entre 1 e p^n são primos de p^n. Assim, como afirmado:

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

11.43 Encontre: (a) $\phi(81)$, $\phi(7^6)$; (b) $\phi(72)$, $\phi(3000)$.

(a) De acordo com o Problema 11.42,

$$\phi(81) = \phi(3^4) = 3^3(3-1) = 27(2) = 54 \quad \text{e} \quad \phi(7^6) = 7^5(7-1) = 6(7^5)$$

(b) Use o Teorema 11.25, que estabelece que ϕ é multiplicativa:

$$\phi(72) = \phi(3^2 \cdot 2^3) = \phi(3^2)\phi(2^3) = 3(3-1) \cdot 2^2(2-1) = 24$$
$$\phi(3000) = \phi(3 \cdot 2^2 \cdot 5^3) = \phi(3)\phi(2^2)\phi(5^3) = 2 \cdot 2 \cdot 5^2(5-1) = 400$$

11.44 Demonstre o Teorema 11.25: Se a e b são primos entre si, então $\phi(ab) = \phi(a)\,\phi(b)$.

Sejam a e b inteiros positivos coprimos (primos entre si), e seja S o conjunto de números de 1 a ab dispostos em um array como na Fig. 11-7. Ou seja, a primeira linha de S é a lista de números de 1 a a, a segunda linha é a lista de números de $a + 1$ a $2a$, e assim por diante. Como a e b são coprimos, qualquer inteiro x é coprimo de ab se, e somente se, é coprimo de ambos a e b. Encontramos a quantia de tais inteiros x no array S.

Uma vez que $na + k \equiv k \pmod{a}$, cada coluna de S pertence à mesma classe de resíduos módulo a. Portanto, qualquer inteiro x de S é coprimo de a se, e somente se, x pertence a uma coluna encabeçada por algum inteiro k que é coprimo de a. Por outro lado, existem $\phi(a)$ colunas desse tipo, pois a primeira linha é um sistema de resíduos módulo a.

$$\begin{array}{ccccccc}
1 & 2 & 3 & \ldots & k & \ldots & a \\
a+1 & a+2 & a+3 & \ldots & a+k & \ldots & 2a \\
2a+1 & 2a+2 & 2a+3 & \ldots & 2a+k & \ldots & 3a \\
\\
(b-1)a+1 & & & & (b-1)a+k & \ldots & ba
\end{array}$$

Figura 11-7

Consideremos agora uma coluna arbitrária no array S que consiste nos números.

$$k \quad a+k \quad 2a+k \quad 3a+k \quad \ldots \quad (b-1)a+k$$

De acordo com o Problema 11.10, esses b inteiros formam um sistema de resíduos módulo b, ou seja, não há inteiros congruentes módulo b tomados dois a dois. Logo, (11.11) contém exatamente ϕ (b) inteiros que são coprimos de b. Mostramos que o array b contém colunas consistindo nos inteiros que são coprimos de ϕ (a), e que cada coluna contém ϕ (b) inteiros que são coprimos de b. Assim, existem ϕ (a) ϕ (b) inteiros no array S que são coprimos de ambos a e b e, portanto, coprimos de ab. Logo, como pedido,

$$\phi(ab) = \phi(a)\phi(b)$$

Aritmética módulo m, $\mathbf{Z}_m$

11.45 Exiba as tabuadas de adição e multiplicação para: (a) $\mathbf{Z}_4$; (b) $\mathbf{Z}_7$

(a) Ver Fig. 11-8. (b) Ver Fig. 11-9

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0		2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Figura 11-8

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0		2	3
5	5	6	0		2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Figura 11-9

11.46 Em $\mathbf{Z}_{11}$, encontre: (a) $-2, -5, -9, -10$; (b) $2/7, 3/7, 5/7, 8/7, 10/7, 1/7$.

(a) Note que $-a = m - a$, uma vez que $(m - a) + a = 0$. Portanto:

$$-2 = 11 - 2 = 9, \quad -5 = 11 - 5 = 6, \quad -9 = 11 - 9 = 2, \quad -10 = 11 - 10 = 1$$

(b) Por definição, a/b é o inteiro c tal que $bc = a$. Como estamos dividindo por 7, primeiro, compute a tabuada de multiplicação para 7 em $\mathbf{Z}_{11}$, como na Fig. 11-10. Agora, encontre o número na tabuada e a resposta estará acima desse número. Assim:

×	0	1	2	3	4	5	6	7	8	9	10
7	0	7	3	10	6	2	9	5	1	8	4

Figura 11-10

$$2/7 = 5, \quad 3/7 = 2, \quad 5/7 = 7, \quad 8/7 = 9, \quad 10/7 = 3, \quad 1/7 = 8$$

Note que $7^{-1} = 8$, pois $7(8) = 8(7) = 1$.

11.47 Considere $\mathbf{Z}_p$, onde p é primo. Prove que:

(a) Se $ab = ac$ e $a \neq 0$, então $b = c$;

(b) Se $ab = 0$, então $a = 0$ ou $b = 0$.

(a) Se $ab = ac$ em $\mathbf{Z}_p$, então $ab \equiv ac \pmod p$. Como $a \neq 0$, $\text{mdc}(a, p) = 1$. De acordo com o Teorema 11.23, podemos cancelar os a's para obter $b \equiv c \pmod p$. Portanto, $b = c$ em $\mathbf{Z}_p$.

(b) Se $ab = 0$ em $\mathbf{Z}_p$, então $ab \equiv 0 \pmod p$. Logo, p divide o produto ab. Como p é um primo, $p \mid a$ ou $p \mid b$, ou seja, $a \equiv 0 \pmod p$ ou $b \equiv 0 \pmod p$. Logo, $a = 0$ ou $b = 0$ em $\mathbf{Z}_p$.

11.48 Considere $a \neq 0$ em $\mathbf{Z}_m$, onde $\text{mdc}(a, m) = 1$. Mostre que a admite um inverso multiplicativo em $\mathbf{Z}_m$.

Como $a \neq 0$ e $\text{mdc}(a, m) = 1$, existem inteiros x e y tais que $ax + my = 1$ ou $ax - 1 = my$. Assim, m divide $ax - 1$ e, portanto, $ax \equiv 1 \pmod m$. Reduza x módulo m a um elemento x' em $\mathbf{Z}_m$. Então, $ax' = 1$ em $\mathbf{Z}_m$.

11.49 Encontre a^{-1} em $\mathbf{Z}_m$, onde: (a) $a = 37$ e $m = 249$; (b) $a = 15$ e $m = 234$.

(a) Primeiro determine $d = \text{mdc}(37, 249)$, obtendo $d = 1$. Em seguida, como no Exemplo 11.6, encontre x e y tais que $ax + my = 1$. Isso conduz a $x = -74$ e $y = 14$. Ou seja,

$$-74(37) + 11(249) = 1 \quad \text{e, assim,} \quad -74(37) \equiv 1 \pmod{249}$$

Adicione $m = 249$ a -74 para obter $-74 + 249 = 175$. Logo, $(175)(37) \equiv 1 \pmod{249}$.

Consequentemente, $a^{-1} = 175$ em $\mathbf{Z}_{249}$.

(b) Primeiro encontre $d = \text{mdc}(15, 234)$, obtendo $d = 3$. Logo, $d \neq 1$ e, portanto, 15 não admite inverso multiplicativo em $\mathbf{Z}_{234}$.

11.50 Para os seguintes polinômios sobre $\mathbf{Z}_7$, determine: (a) $f(x) + g(x)$ e (b) $f(x)h(x)$.

$$f(x) = 6x^3 - 5x^2 + 2x - 4 \qquad g(x) = 5x^3 + 2x^2 + 6x - 1 \qquad h(x) = 3x^2 - 2x - 5$$

Realize as operações como se os polinômios fossem definidos sobre os inteiros $\mathbf{Z}$ e, em seguida, reduza os coeficientes módulo 7.

(a) Temos $f(x) + g(x) = 11x^3 - 3x^2 + 8x - 5 = 4x^3 - 3x^2 + x - 5 = 4x^3 + 4x^2 + x + 2$

(b) Primeiro, determine o produto $f(x)h(x)$ como na Fig. 11-11. Depois, reduza módulo 7 para obter

$$f(x)h(x) = 4x^5 - 6x^4 + 2x^2 - 2x + 6 = 4x^5 + x^4 + 2x^2 + 5x + 6$$

$$\begin{array}{r}
6x^3 - 5x^2 + 2x - 4 \\
3x^2 - 2x - 5 \\
\hline
18x^5 - 15x^4 + 6x^3 - 12x^2 \\
-12x^4 + 10x^3 - 4x^2 + 8x \\
-30x^3 + 25x^2 - 10x + 20 \\
\hline
18x^5 - 27x^4 - 14x^3 + 9x^2 - 2x + 20
\end{array}$$

Figura 11-11

Equações de congruência

11.51 Resolva a equação de congruência $f(x) = 4x^4 - 3x^3 + 2x^2 + 5x - 4 \equiv 0 \pmod 6$.

Como a equação é não linear, resolvemos a equação, testando os números em um sistema completo de resíduos módulo 6, digamos, $\{0, 1, 2, 3, 4, 5\}$. Temos:

$$f(0) = -4 \not\equiv 0 \pmod 6, \quad f(2) = 54 \equiv 0 \pmod 6, \quad f(4) = 880 \equiv 4 \not\equiv 0 \pmod 6$$
$$f(1) = 4 \not\equiv 0 \pmod 6, \quad f(3) = 272 \equiv 2 \not\equiv 0 \pmod 6, \quad f(5) = 2196 \equiv 0 \pmod 6$$

Assim, apenas 2 e 5 são raízes de $f(x)$ módulo 6. Isto é, $\{2, 5\}$ é um conjunto completo de soluções.

11.52 Resolva a equação de congruência $f(x) = 26x^4 - 31x^3 + 46x^2 - 76x + 57 \equiv 0 \pmod 8$.

Primeiro, reduzimos os coeficientes de $f(x)$ módulo 8 para obter a equação de congruência equivalente

$$g(x) = 2x^4 - 7x^3 + 6x^2 - 4x + 1 \equiv 0 \pmod 8$$

Como $7 \equiv -1 \pmod 8$ e $6 \equiv -2 \pmod 8$, podemos simplificar mais nossa equação original para obter a equação de congruência equivalente

$$h(x) = 2x^4 + x^3 - 2x^2 - 4x + 1 \equiv 0 \pmod 8$$

Testamos os números em um sistema completo de resíduos módulo 8 e, para manter nossas contas tão simples quanto possível, escolhemos $\{-3, -2, -1, 0, 1, 2, 3, 4\}$. (Ou seja, escolhemos os numeros cujos valores absolutos são mínimos.) Substituindo esses números em $h(x)$, temos:

$$h(-3) = 130 \equiv 2 \pmod 8, \quad h(0) = 1 \equiv 1 \pmod 8, \quad h(3) = 160 \equiv 0 \pmod 8$$
$$h(-2) = 9 \equiv 1 \pmod 8, \quad h(1) = -2 \equiv 6 \pmod 8, \quad h(4) = 529 \equiv 1 \pmod 8$$
$$h(-1) = -4 \equiv 4 \pmod 8, \quad h(2) = 25 \equiv 1 \pmod 8,$$

Logo, 3 é a única solução de $f(x) \pmod 8$.

11.53 Resolva cada equação de congruência linear:

(a) $3x \equiv 2 \pmod 8$; (b) $6x \equiv 5 \pmod 9$; (c) $4x \equiv 6 \pmod{10}$

Como os módulos são relativamente pequenos, encontramos todas as soluções por teste. Lembre que $ax \equiv b \pmod m$ tem exatamente $d = \text{mdc}(a, m)$ soluções, desde que d divida b.

(a) Aqui $\text{mdc}(3, 8) = 1$, logo a equação admite uma única solução. Testando 0, 1, 2, ..., 7, descobrimos que $3(6) = 18 \equiv 2 \pmod 8$. Portanto, 6 é a única solução.

(b) Aqui $\text{mdc}(6, 9) = 3$; mas 3 não divide 5. Logo, o sistema não tem solução.

(c) Aqui $\text{mdc}(4, 10) = 2$ e 2 divide 6, portanto, o sistema tem duas soluções. Testando 0, 1, 2, ..., 9, percebemos que

$$4(4) = 16 \equiv 6 \pmod{10} \quad \text{e} \quad 4(9) = 36 \equiv 6 \pmod{10}$$

Então 4 e 9 são nossas duas soluções.

11.54 Resolva a equação de congruência $1092x \equiv 213 \pmod{2295}$.

Testar não é uma maneira eficiente de resolver essa equação, uma vez que o módulo $m = 2295$ é grande. Primeiro, usamos o algoritmo euclidiano para encontrar $d = \text{mdc}(1092, 2295) = 3$. Dividindo 213 por $d = 3$, temos 0 como resto, ou seja, 3 divide 213. Logo, a equação tem três soluções (incongruentes).

Divida a equação e o módulo $m = 2295$ por $d = 3$, para obter a equação de congruência

$$364x \equiv 71 \pmod{765} \tag{11.12}$$

Sabemos que 364 e 796 são primos entre si, uma vez que dividimos por $d = \text{mdc}(1092, 2295) = 3$, logo, a equação (11.12) tem solução única módulo 765. Resolvemos (11.12), encontrando primeiro a solução da equação

$$364x \equiv 1 \pmod{765} \tag{11.13}$$

Essa solução é obtida, determinando s e t tais que

$$364s + 765t = 1$$

Usando o algoritmo euclidiano e "revelando" como no exemplo 11.6 e no Problema 11.21, obtemos $s = 124$ e $t = -59$. Consequentemente, $s = 124$ é a solução única de (11.13). Multiplicando essa solução $s = 124$ por 71 e reduzindo o módulo 765, obtemos

$$124(71) = 8804 \equiv 389 \pmod{765}$$

Essa é a solução única de (11.12).

Por último, adicionamos o novo módulo $m = 765$ à solução $x_1 = 389$ duas vezes, para obter as outras duas soluções da equação dada:

$$x_2 = 389 + 765 = 1154, \quad x_3 = 1154 + 765 = 1919$$

Em outras palavras, $x_1 = 389$, $x_2 = 1154$ e $x_3 = 1919$ formam um conjunto completo de soluções da equação de congruência dada $1092x \equiv 213 \pmod{2295}$.

11.55 **Resolva a equação de congruência $455x \equiv 204 \pmod{469}$.**

Primeiro, use o algoritmo euclidiano para determinar $d = \text{mdc}(455, 469) = 7$. Dividindo 204 por $d = 7$, temos 1 como resto; isto é, 7 não divide 204. Logo, a equação não admite solução.

11.56 **Encontre o menor inteiro positivo x tal que x dividido por 3 resulta em resto 2, dividido por 7 resulta em resto 4 e dividido por 10 tem resto 6.**

Buscamos pela menor solução positiva comum das três equações de congruência:

$$(a)\ x \equiv 2 \pmod{3}; \quad (b)\ x \equiv 4 \pmod{7}; \quad (c)\ x \equiv 6 \pmod{10}$$

Observe que os módulos 3, 7 e 10 são primos entre si, se tomados dois a dois. O Teorema Chinês do Resto (TCR), Teorema 11.29, nos diz que existe uma única solução módulo produto $m = 3(7)(10) = 210$. Resolvemos os problemas de duas maneiras.

Método 1: Primeiro, aplicamos TCR às duas primeiras equações,

$$(a)\ x \equiv 2 \pmod{3} \quad \text{e} \quad (b)\ x \equiv 4 \pmod{7}$$

Sabemos haver uma única solução módulo $M = 3 \cdot 7 = 21$. Adicionando múltiplos do módulo $m = 7$ à solução dada $x = 4$ da segunda equação (b), obtemos as três soluções de (b) que são menores do que 21

$$4, 11, 18$$

Testando cada uma dessas soluções de (b) na primeira equação (a), descobrimos que 11 é a única solução de ambas as equações.

Agora aplicamos o mesmo processo às duas equações

$$(c)\ x \equiv 6 \pmod{10} \quad \text{e} \quad (d)\ x \equiv 11 \pmod{21}$$

O TCR nos diz que existe uma única solução módulo $M = 21 \cdot 10 = 210$. Adicionando múltiplos do módulo $m = 21$ à solução dada $x = 11$ da equação (d), conseguimos as 10 soluções de (d) que são menores do que 210.

$$11, 32, 53, 74, 95, 116, 137, 158, 179, 210$$

Testando cada uma dessas soluções de (d) na equação (c), descobrimos que $x = 116$ é a única solução da equação (c). Consequentemente, $x = 116$ é o menor inteiro positivo satisfazendo as três equações dadas, (a), (b) e (c).

Método 2: Usando a notação da Proposição 11.30, obtemos

$$M = 3 \cdot 7 \cdot 10 = 210, \quad M_1 = 210/3 = 70, \quad M_2 = 210/7 = 30, \quad M_3 = 210/10 = 21$$

Buscamos agora soluções para as equações

$$70x \equiv 1 \pmod{3}, \quad 30x \equiv 1 \pmod{7}, \quad 21x \equiv 1 \pmod{10}$$

Reduzindo 70 módulo 3, 30 módulo 7 e 21 módulo 10, conseguimos o sistema equivalente

$$x \equiv 1 \pmod{3}, \quad 2x \equiv 1 \pmod{7}, \quad x \equiv 1 \pmod{10}$$

As soluções dessas três equações são, respectivamente,

$$s_1 = 1, \quad s_2 = 4, \quad s_3 = 1$$

Substituindo na fórmula

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

obtemos a seguinte solução de nosso sistema original.

$$x_0 = 70 \cdot 1 \cdot 2 + 30 \cdot 4 \cdot 4 + 21 \cdot 1 \cdot 6 = 746$$

Dividindo essa solução pelo módulo $M = 210$, temos o resto $x = 116$, que é a única solução do sistema original entre 0 e 210.

11.57 **Prove o Teorema 11.26: Se a e m são primos entre si, então $ax \equiv 1 \pmod{m}$ tem uma única solução, caso contrário, não admite solução.**

Suponha que x_0 é uma solução. Então m divide $ax_0 - 1$ e, portanto, existe y_0 tal que $my_0 = ax_0 - 1$. Logo,

$$ax_0 + my_0 = 1 \tag{11.14}$$

e a e m são coprimos (primos entre si). Reciprocamente, se a e m são coprimos, então existem x_0 e y_0 satisfazendo (11.14), o que implica que x_0 é uma solução de $ax \equiv 1 \pmod{m}$.

Resta provar que x_0 é uma solução única módulo m. Suponha que x_1 é outra solução. Então

$$ax_0 \equiv 1 \equiv ax_1 \pmod{m}$$

Como a e m são coprimos, a Lei Modificada de Cancelamento vale aqui. Portanto,

$$x_0 \equiv x_1 \pmod{m}$$

Assim, o teorema está demonstrado.

11.58 **Demonstre o Teorema 11.27: Suponha que a e m são primos entre si. Então $ax \equiv b \pmod{m}$ tem uma única solução. Além disso, se s é a solução única de $ax \equiv 1 \pmod{m}$, então $x = bs$ é a única solução de $ax \equiv b \pmod{m}$.**

De acordo com o Teorema 11.26 (provado no Problema 11.57), existe uma solução única s de $ax \equiv 1 \pmod{m}$. Então, $as \equiv 1 \pmod{m}$ e, assim,

$$a(bs) = (as)b \equiv 1 \cdot b = b \pmod{m}$$

Ou seja, $x = bs$ é uma solução de $ax \equiv b \pmod{m}$. Suponha que x_0 e x_1 são duas dessas soluções. Então

$$ax_0 \equiv b \equiv ax_1 \pmod{m}$$

Como a e m são primos entre si, a Lei Modificada de Cancelamento nos diz que $x_0 \equiv x_1 \pmod{m}$. Ou seja, $ax \equiv b \pmod{m}$ tem uma única solução módulo m.

11.59 **Prove o Teorema 11.28: Considere a equação a seguir, onde $d = \text{mdc}(a, m)$.**

$$ax \equiv b \pmod{m} \tag{11.15}$$

(i) Suponha que d não divida b. Então, (11.15) não admite solução.

(ii) Suponha que d divida b. Então, (11.15) tem d soluções, as quais são todas congruentes módulo M à solução única da seguinte equação, onde $A = a/d$, $B = b/d$, $M = m/d$:

$$Ax \equiv B \pmod{M} \tag{11.16}$$

(i) Suponha que x_0 é uma solução de (11.15). Então, $ax_0 \equiv b \pmod{m}$ e, assim, m divide $ax_0 - b$. Portanto, existe um inteiro y_0 tal que $my_0 = ax_0 - b$ ou $my_0 + ax_0 = b$. Mas $d = \text{mdc}(a, m)$ e, logo, d divide $my_0 + ax_0$. Ou seja, d divide b. Consequentemente, se d não divide b, então não existe solução.

(ii) Suponha que x_0 é uma solução de (11.15). Então, como discutido acima,

$$my_0 + ax_0 = b$$

Dividindo por d, temos (11.16). Logo, M divide $Ax_0 - B$ e, assim, x_0 é uma solução de (11.16). Reciprocamente, suponha que x_1 é uma solução de (11.16). Então, como visto acima, existe um inteiro y_1 tal que

$$My_1 + Ax_1 = B$$

Multiplicando por d, temos

$$dMy_1 + dAx_1 = dB \quad \text{ou} \quad my_1 + ax_1 = b$$

Portanto, m divide $ax_1 - b$, quando x_1 é uma solução de (11.15). Assim, (11.16) tem a mesma solução inteira. Seja x_0 a menor solução positiva de (11.16). Visto que $m = dM$,

$$x_0, \quad x_0 + M, \quad x_0 + 2M, \quad x_0 + 3M, \quad \ldots, \quad x_0 + (d-1)M$$

são precisamente a solução de (11.16) e de (11.15) entre 0 e m. Logo, (11.15) tem d soluções módulo m e todas são congruentes a x_0 módulo M.

11.60 **Prove o Teorema Chinês do Resto (Teorema 11.29), dado o sistema**

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \quad \ldots, \quad x \equiv r_k \pmod{m_k} \tag{11.17}$$

onde os m_i são primos entre si, se tomados dois a dois. Então o sistema tem uma única solução módulo $M = m_1 m_2 \cdots m_k$.

Considere o inteiro

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

onde $M_i = M/m_i$ e s_i é a única solução de $M_i x \equiv 1 \pmod{m_i}$. Seja j dado.

Para $i \neq j$, temos $m_j \mid M_i$ e, portanto,

$$M_i s_i r_i \equiv 0 \pmod{m_j}$$

Por outro lado, $M_j S_j \equiv 1 \pmod{m_j}$; e, assim,

$$M_j s_j r_j \equiv r_j \pmod{m_j}$$

Consequentemente,

$$x_0 \equiv 0 + \cdots + 0 + r_j + 0 + \cdots + 0 \equiv r_j \pmod{m_j}$$

Em outras palavras, x_0 é uma solução de cada uma das equações em (11.17).

Ou seja, x_0 é a única solução do sistema (11.17), módulo M.

Suponha que x_1 é outra solução de todas as equações em (11.17). Então:

$$x_0 \equiv x_1 \pmod{m_1}, \quad x_0 \equiv x_1 \pmod{m_2}, \quad \cdots, \quad x_0 \equiv x_1 \pmod{m_k}$$

Logo, $m_i \mid (x_0 - x_1)$, para cada i. Como os m_i são primos entre si, $M = \text{mmc}(m_1, m_2, \ldots, m_k)$ e, portanto, $M \mid (x_0 - x_1)$. Isto é, $x_0 = x_1 \pmod{M}$. Logo, o teorema está provado.

Problemas Complementares

Ordem e desigualdades, valor absoluto

11.61 Insira o símbolo correto, $<$, $>$ ou $=$, entre cada par de inteiros:

(a) 2 ___ -6; (c) -7 ___ 3; (e) 2^3 ___ 11; (g) -2 ___ -7;

(b) -3 ___ -5; (d) -8 ___ -1; (f) 2^3 ___ -9; (h) 4 ___ 9.

11.62 Calcule: (a) $|3 - 7|$, $|-3 + 7|$, $|-3 - 7|$, (b) $|2 - 5| + |3 + 7|$, $|1 - 4| - |2 - 9|$, (c) $||5 - 9| + |2 - 3||$, $||-6 - 2| - |2 - 6||$

11.63 Encontre a distância d entre cada par de inteiros. (a) 2 e -5, (b) -6 e 3, (c) 2 e 8, (d) -7 e -1, (e) 3 e -3, (f) -7 e -9.

11.64 Encontre todos os inteiros n tais que: (a) $3 < 2n - 4 < 10$; (b) $1 < 6 - 3n < 13$.

11.65 Demonstre a Proposição 11.1: (i) $a \leq a$, para qualquer inteiro a; (ii) Se $a \leq b$ e $b \leq a$, então $a = b$.

11.66 Demonstre a Proposição 11.2: Para quaisquer inteiros a e b, exatamente uma das afirmações a seguir vale: $a < b$, $a = b$ ou $a > b$.

11.67 Prove: (a) $2ab \leq a^2 + b^2$; (b) $ab + ac + bc \leq a^2 + b^2 + c^2$.

11.68 Proposição 11.4 (i) $|a| \geq 0$, e $|a| = 0$ sss $a = 0$; (ii) $-|a| \leq a \leq |a|$; (iii) $||a| - |b|| \leq |a \pm b|$

11.69 Mostre que $a - xb \geq 0$ se $b \neq 0$, e $x = -|a|b$.

Indução matemática, princípio da boa ordem

11.70 Prove a proposição de que a soma dos n primeiros inteiros pares é $n(n + 1)$, ou seja,

$$P(n): 2 + 4 + 6 + \cdots + 2n = n(n + 1).$$

11.71 Prove que a soma dos primeiros n cubos é igual ao quadrado da soma dos primeiros n inteiros positivos:

$$P(n): 1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

11.72 Prove: $1 + 4 + 7 + \cdots + (3n - 2) = n(3n - 1)/2$

11.73 Prove: (a) $a^n a^m = a^{n+m}$; (b) $(a^n)^m = a^{nm}$; (c) $(ab)^n = a^n b^n$

11.74 Prove: $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$

11.75 Prove: $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$

11.76 Prove: $\frac{1^2}{1 \cdot 3} + \frac{2^2}{3 \cdot 5} + \frac{3^2}{5 \cdot 7} + \cdots + \frac{n^2}{(2n-1)(2n+1)} = \frac{n(n+1)}{2(2n+1)}$

11.77 Prove: $x^{n+1} - y^{n+1} = (x - y)(x^n + x^{n-1}y + x^{n-2}y^2 + \cdots + y^n)$

11.78 Prove $|P(A)| = 2^n$, onde $|A| = n$. (Aqui $P(A)$ é o conjunto potência do conjunto A com n elementos.)

Algoritmo de divisão

11.79 Para cada par de inteiros a e b, determine inteiros q e r tais que $a = bq + r$ e $0 \leq r < |b|$

(a) $a = 608$ e $b = -17$; (b) $a = -278$ e $b = 12$; (c) $a = -417$ e $b = -8$.

11.80 Prove cada uma das seguintes afirmações.

(a) Qualquer inteiro a é da forma $5k$, $5k + 1$, $5k + 2$, $5k + 3$ ou $5k + 4$.

(b) Um de cada cinco inteiros consecutivos é múltiplo de 5.

11.81 Demonstre cada uma das seguintes afirmações.

(a) O produto de quaisquer três inteiros consecutivos é divisível por 6.

(b) O produto de quaisquer quatro inteiros consecutivos é divisível por 24.

11.82 Mostre que cada um dos números a seguir não é racional: (a) $\sqrt{3}$; (b) $\sqrt[3]{2}$.

11.83 Mostre que $\sqrt{p}$ não é racional, onde p é qualquer número primo.

Divisibilidade, máximo divisor comum, primos

11.84 Encontre todos os possíveis divisores de: (a) 24, (b) $19\,683 = 3^9$, (c) $432 = 2^4 \cdot 3^3$.

11.85 Liste todos os números primos entre 100 e 150.

11.86 Expresse como um produto de números primos: (a) 2940; (b) 1485; (c) 8712; (d) 319 410

11.87 Para cada par de inteiros a e b, encontre $d = \text{mdc}(a, b)$ e determine m e n tais que $d = ma + nb$:

(a) $a = 356, b = 48$; (b) $a = 1287, b = 165$; (c) $a = 2310, b = 168$; (d) $a = 195, b = 968$;
(e) $a = 249, b = 37$.

11.88 Encontre: (a) mmc(5, 7); (b) mmc(3, 33); (c) mmc(12, 28).

11.89 Suponha que $a = 5880$ e $b = 8316$. (a) Expresse a e b como produtos de primos. (b) Determine $\text{mdc}(a, b)$ e $\text{mmc}(a, b)$. (c) Verifique que $\text{mmc}(a, b) = |ab|/\text{mdc}(a, b)$.

11.90 Prove que: (a) Se $a \mid b$, então (i) $a \mid -b$, (ii) $-a \mid b$, (iii) $-a \mid -b$. (b) Se $ab \mid ac$, então $b \mid c$.

11.91 Prove que: (a) Se $n > 1$ é composto, então n tem um divisor positivo d tal que $d \leq \sqrt{n}$. (b) Se $n > 1$ não é divisível por um primo $p \leq \sqrt{n}$, então n é primo.

11.92 Prove que: (a) Se $am + bn = 1$, então $\text{mdc}(a, b) = 1$. (b) Se $a = bq + r$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$.

11.93 Prove que: (a) $\text{mdc}(a, a + k)$ divide k; (b) $\text{mdc}(a, a + 2)$ é igual a 1 ou 2.

11.94 Prove que: (a) Se $a > 2$ e $k > 1$, então $a^k - 1$ é composto. (b) Se $n > 0$ e $2^n - 1$ é primo, então n é primo.

11.95 Seja n um inteiro positivo. Demonstre que:

(a) 3 divide n se, e somente se, 3 divide a soma dos dígitos de n.

(b) 9 divide n se, e somente se, 9 divide a soma dos dígitos de n.

(c) 8 divide n se, e somente se, 8 divide o inteiro formado pelos três últimos dígitos de n.

11.96 Estenda as definições de mdc e mmc para quaisquer conjuntos finitos de inteiros, ou seja, para inteiros $a_1, a_2, \ldots, a_k$, defina: (a) $\text{mdc}(a_1, a_2, \ldots, a_k)$; (b) $\text{mmc}(a_1, a_2, \ldots, a_k)$.

11.97 Prove que: Se $a_1 \mid n, a_2 \mid n, \ldots, a_k \mid n$, então $m \mid n$, onde $m = \text{mmc}(a_1, a_2, \ldots, a_k)$

11.98 Prove que: Existem lacunas arbitrariamente grandes entre números primos, isto é, para qualquer inteiro positivo k, existem k inteiros compostos (não primos) consecutivos.

Congruências

11.99 Quais dos seguintes itens são verdadeiros?

(a) $224 \equiv 762 \pmod 8$, (b) $582 \equiv 263 \pmod{11}$, (c) $156 \equiv 369 \pmod 7$, (d) $-238 \equiv 483 \pmod{13}$.

11.100 Encontre o menor inteiro não negativo que seja congruente módulo $m = 9$ a cada um dos números a seguir: (a) 457; (b) 1578; (c) -366; (d) -3288. (O inteiro deve estar no conjunto $\{0, 1, 2, \ldots, 7, 8\}$.)

11.101 Determine o menor inteiro em valor absoluto que seja congruente módulo $m = 9$ a cada um dos números a seguir: (a) 511, (b) 1329; (c) -625; (d) -2717. (O inteiro deve estar no conjunto $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$).

11.102 Encontre todos os números entre 1 e 100 que são congruentes a 4 módulo $m = 11$.

11.103 Determine todos os números entre -50 e 50 que são congruentes a 12 módulo $m = 9$.

Sistemas de resíduos, função phi de Euler ϕ

11.104 Para cada módulo m, exiba dois sistemas completos de resíduos, um consistindo nos menores inteiros não negativos e o outro consistindo nos inteiros com os menores valores absolutos: (a) $m = 11$; (b) $m = 14$

11.105 Exiba um sistema reduzido de resíduos módulo m e encontre $\phi(m)$, onde (a) $m = 4$, (b) $m = 11$, (c) $m = 14$, (d) $m = 15$

11.106 Exiba um sistema completo de resíduos módulo $m = 8$, consistindo inteiramente em: (a) múltiplos de 5, (b) potências de 3.

11.107 Mostre que $\{1^2, 2^2, 3^2, \ldots, m^2\}$ não é um sistema completo de resíduos módulo m para $m > 2$.

11.108 Encontre. (a) $\phi(10)$; (b) $\phi(12)$, (c) $\phi(15)$; (d) $\phi(3^7)$, (e) $\phi(5^6)$, (f) $\phi(2^4\ 7^6\ 13^3)$.

11.109 Determine o número s de inteiros positivos menores do que 3200 que são coprimos de 8000.

11.110 Considere uma coluna arbitrária no array S da Fig. 11-7 que consiste nos números.

$$k,\ a + k,\ 2a + k,\ 3a + k,\ \ldots,\ (b - 1)a + k$$

Mostre que esses b inteiros formam um sistema de resíduos módulo b.

Aritmética módulo m, Z_m

11.111 Exiba as tabuadas de adição e multiplicação para. (a) $\mathbf{Z}_2$; (b) $\mathbf{Z}_8$.

11.112 Em $\mathbf{Z}_{13}$, encontre: (a) $-2, -3, -5, -9, -10, -11$; (b) $2/9, 4/9, 5/9, 7/9, 8/9$.

11.113 Em $\mathbf{Z}_{17}$, encontre: (a) $-3, -5, -6, -8, -13, -15, -16$; (b) $3/8, 5/8, 7/8, 13/8, 15/8$

11.114 Determine a^{-1} em $\mathbf{Z}_m$, onde. (a) $a = 15, m = 127$, (b) $a = 61, m = 124$, (c) $a = 12, m = 111$

11.115 Encontre o produto $f(x)g(x)$ para os seguintes polinômios definidos sobre $\mathbf{Z}_5$

$$f(x) = 4x^3 - 2x^2 + 3x - 1,\quad g(x) = 3x^2 - x - 4$$

Equações de congruência

11.116 Resolva cada equação de congruência.

(a) $f(x) = 2x^3 - x^2 + 3x + 1 \equiv 0 \pmod 5$
(b) $g(x) = 3x^4 - 2x^3 + 5x^2 + x + 2 \equiv 0 \pmod 7$
(c) $h(x) = 45x^3 - 37x^2 + 26x + 312 \equiv 0 \pmod 6$

11.117 Resolva cada equação linear de congruência.

(a) $7x \equiv 3 \pmod 9$; (b) $4x \equiv 6 \pmod{14}$; (c) $6x \equiv 4 \pmod 9$.

11.118 Resolva cada equação linear de congruência.

(a) $5x \equiv 3 \pmod 8$; (b) $6x \equiv 9 \pmod{16}$; (c) $9x \equiv 12 \pmod{21}$.

11.119 Resolva cada equação linear de congruência. (a) $37x \equiv 1 \pmod{249}$; (b) $195x \equiv 23 \pmod{968}$.

11.120 Resolva cada equação linear de congruência. (a) $132x \equiv 169 \pmod{735}$; (b) $48x \equiv 284 \pmod{356}$.

11.121 Um teatro de marionetes tem apenas 60 cadeiras. A entrada no teatro custa \$2,25 por adulto e \$1,00 por criança. Suponha que \$117,25 foi coletado. Encontre o número de adultos e crianças que assistiram à apresentação.

11.122 Um garoto vende maçãs a 12 centavos cada e peras a 7 centavos a unidade. Suponha que o garoto faturou \$3,21. Encontre o número de maçãs e de peras que ele vendeu.

11.123 Determine a menor solução positiva de cada sistema de equações de congruência

(a) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod{11}$
(b) $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$, $x \equiv 6 \pmod 9$
(c) $x \equiv 5 \pmod{45}$, $x \equiv 6 \pmod{49}$, $x \equiv 7 \pmod{52}$

Respostas dos Problemas Complementares

11.61 (a) $2 > -6$; (b) $-3 > -5$; (c) $-7 < 3$, (d) $-8 < -1$, (e) $2^3 < 11$, (f) $2^3 > -9$; (g) $-2 > -7$, (h) $4 > -9$

11.62 (a) 4, 4, 10; (b) $3 + 10 = 13$, $3 - 7 = -4$; (c) $4 + 1 = 5$, $8 - 4 = 4$.

11.63 (a) 7; (b) 9; (c) 6; (d) 6; (e) 6; (f) 2.

11.64 (a) 4, 5, 6; (b) $-2, -1, 0, 1$

11.79 (a) $q = -15$, $r = 13$; (b) $q = -24$, $r = 10$; (c) $q = 53$, $r = 7$

11.81 (a) Um é divisível por 2 e um é divisível por 3.

(b) Um é divisível por 4, outro é divisível por 2 e um é divisível por 3.

11.84 (a) 1, 2, 3, 4, 6, 8, 12, 24; (b) 3^n para $n = 0$ a 9, (c) 2^r3^s para $r = 0$ a 4 e $s = 0$ a 3.

11.85 101, 103, 107, 109, 113, 127, 131, 137, 139, 149

11.86 (a) $2940 = 2^2 \cdot 3 \cdot 5 \cdot 7^2$; (b) $1485 = 3^3 \cdot 5 \cdot 11$; (c) $8712 = 2^3 \cdot 3^2 \cdot 11^2$, (d) $319\,410 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13^2$.

11.87 (a) $d = 4 = 5(356) - 37(48)$; (b) $d = 33 = 8(165) - 1(1287)$; (c) $d = 42 = 14(168) - 1(2310)$; (d) $d = 1 = 139(195) - 28(968)$; (e) $11(249) - 74(37)$.

11.88 (a) 35, (b) 33; (c) 84.

11.89 (a) $a = 2^3 \cdot 3 \cdot 5 \cdot 7^2$, $b = 2^2 \cdot 3^3 \cdot 7 \cdot 11$; (b) $\text{mdc}(a, b) = 2^2 \cdot 3 \cdot 7$, $\text{mmc}(a, b) = 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11 = 1.164.240$.

11.94 (a) Sugestão: $a^k - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{k-1})$, (b) Sugestão: Se $n = ab$, então $2^n - 1 = (2^a)^b - 1$

11.98 $(k + 1)! + 2$, $(k + 1)! + 3$, $(k + 1)! + 4, \ldots, (k + 1)! + (k + 1)$ são divisíveis por 2, 3, 4, ..., $k + 1$, respectivamente.

11.99 (a) Falso; (b) verdadeiro; (c) falso; (d) falso.

11.100 (a) 7; (b) 3; (c) 3; (d) 6.

11.101 (a) -2; (b) -3, (c) -4; (d) 1.

11.102 4, 15, 26, 37, 48, 59, 70, 81, 92.

11.103 $-42, -33, -24, -15, -6, 3, 12, 21, 30, 39, 48$.

11.104 (a) $\{0, 1, \ldots, 10\}$ e $\{-5, -4, \ldots, -1, 0, 1, \ldots, 4, 5\}$, (b) $\{0, 1, \ldots, 13\}$ e $\{-6, -5, \ldots, -1, 0, 1, \ldots, 6, 7\}$

11.105 (a) $\{1, 3\}$; (b) $\{1, 2, \ldots, 10\}$; (c) $\{1, 3, 5, 9, 11, 13\}$, (d) $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

11.106 (a) $\{5, 10, 15, 20, 25, 30, 35, 40\}$, (b) $\{3, 9, 27, 81, 243, 729, 2187, 6561\}$

11.107 $m - 1 \equiv -1 \pmod m$ e, assim, $(m - 1)^2 \equiv 1 \pmod m$.

11.108 (a) 4; (b) 4; (c) $= 8$; (d) $2(3^6)$; (e) $4(5^5)$; (f) $(2^3)(6 \cdot 7^5)(12 \cdot 13^2)$.

11.109 $\phi(8000) = \phi(2^5 \cdot 5^2) = 2^4 \cdot 4 \cdot 5 = 320$. Logo, $s = 4(320) = 1280$.

11.112 (a) 11, 10, 8, 4, 3, 2; (b) 6, 12, 2, 8, 11.

11.113 (a) 14, 12, 11, 9, 4, 2; (b) 11, 7, 3, 8, 4.

11.114 (a) 17; (b) 61; (c) a^{-1} não existe.

11.115 $2x^5 + 2x^2 - x + 4$.

11.116 (a) 1, 3, 4, (b) $2, -2$, (c) $0, 2, 3, -1$.

11.117 (a) 3, (b) 5, 12, (c) sem solução.

11.118 (a) 7, (b) sem solução; (c) 6, 13, 20.

11.119 (a) 175; (b) 293

11.120 (a) Sem solução; (b) 43, 132, 221; 310.

11.121 49 adultos, 7 crianças.

11.122 25 maçãs, 3 peras; 18 maçãs, 15 peras; 11 maçãs, 27 peras; ou 4 maçãs, 39 peras.

11.123 (a) 158, (b) 1.123, (c) 31.415.

Linguagens, Autômatos, Gramáticas

12.1 INTRODUÇÃO

Este capítulo discute três tópicos *linguagens*, *autômatos* e *gramáticas*. Tais tópicos estão intimamente relacionados entre si. Nossas linguagens serão as letras a, b, ... para codificar dados, em vez dos dígitos 0 e 1, usados por outros textos.

12.2 ALFABETO, PALAVRAS E SEMIGRUPO LIVRE

Considere um conjunto A de símbolos não vazio. Uma *palavra* ou *string* no conjunto A é uma sequência finita de seus elementos. Por exemplo, suponha que $A = \{a, b, c\}$ Então, as sequências a seguir são palavras em A

$$u = ababb \text{ e } v = accbaaa$$

Quando discutimos sobre palavras em A, frequentemente chamamos A de *alfabeto*, e seus elementos, de *letras* Também abreviamos nossa notação ao escrever a^2 quando aa, a^3 quando aaa, e assim por diante Portanto, para as palavras acima, $u = abab^2$ e $v = ac^2ba^3$.

A sequência vazia de letras, denotada por λ (a letra grega lâmbda), ou ϵ (a letra grega épsilon), ou 1, é considerada, também, como sendo uma palavra em A, chamada de *palavra vazia.* O conjunto de todas as palavras em A é denotado por A^* (lê-se: "A estrela").

O *comprimento* de uma palavra u, denotada por $|u|$ ou $l(u)$, é o número de elementos na sequência de letras Para as palavras acima u e v, temos $l(u) = 5$ e $l(v) = 7$. Além disso, $l(\lambda) = 0$, onde λ é a palavra vazia.

Observação: A menos que seja dito o contrário, o alfabeto A é finito. Os símbolos u, v e w são reservados para palavras em A, e os elementos de A surgem das letras a, b, c.

Concatenação

Considere duas palavras, u e v, no alfabeto A. A *concatenação* de u e v, escrita uv, é a palavra obtida, ao se escrever as letras de u seguidas das letras de v. Por exemplo, para as palavras acima u e v, temos

$$uv = ababbaccbaaa = abab^2ac^2ba^3$$

Assim como ocorre com as letras, para qualquer palavra u, definimos $u^2 = uu$, $u^3 = uuu$ e, no caso geral, $u^{n+1} = uu^n$

Claramente, para quaisquer palavras u, v e w, as palavras $(uv)w$ e $u(vw)$ são idênticas. Elas apenas consistem em u, v e w escritas em série. Além disso, anexar a palavra vazia antes ou depois de uma palavra u não muda a palavra u. Isto é:

Teorema 12.1: A operação de concatenação para palavras em um alfabeto A é associativa. A palavra vazia λ é um elemento identidade relativamente à operação.

(Em termos gerais, a operação não é comutativa, por exemplo, $uv \neq vu$ para as palavras u e v acima.)

Subpalavras e segmentos iniciais

Considere uma palavra $u = a_1a_2 \ldots a_n$ em um alfabeto A. Qualquer sequência $w = a_j a_{j+1} \ldots a_k$ é chamada de *subpalavra* de u. De modo específico, a subpalavra $w = a_1a_2 \ldots a_k$ que começa com a primeira letra de u é chamada de *segmento inicial* de u. Em outros termos, w é uma subpalavra de u se $u = v_1wv_2$ e w é um segmento inicial de u se $u = wv$. Observe que λ e u são, ambas, subpalavras de uv, uma vez que $u = \lambda u$.

Considere a palavra $u = abca$. As subpalavras e os segmentos iniciais são os que se seguem:

(1) Subpalavras: $\lambda, a, b, c, ab, bc, ca, abc, bca, abca = u$

(2) Segmentos iniciais: $\lambda, a, ab, abc, abca = u$.

Observe que a subpalavra $w = a$ aparece em dois lugares em u. A palavra ac não é uma subpalavra de u, apesar de todas as suas letras pertencerem a u.

Semigrupo livre, monoide livre

Seja F a notação para o conjunto de todas as palavras não vazias de um alfabeto A com a operação de concatenação. Como foi observado acima, a operação é associativa. Logo, F é um semigrupo, ele é chamado de *semigrupo livre sobre A* ou de *semigrupo livre gerado por A*. É fácil mostrar que F satisfaz as leis de cancelamento à esquerda e à direita. Contudo, F não é comutativo quando A possui mais de um elemento. Escrevemos F_A para o semigrupo livre sobre A quando queremos especificar o conjunto A.

Agora, seja $M = A^*$ o conjunto de todas as palavras de A, incluindo a palavra vazia λ. Uma vez que λ é um elemento identidade para a operação de concatenação, M é um monoide, chamado de *monoide livre* sobre A.

12.3 LINGUAGENS

Uma *linguagem L* sobre um alfabeto A é uma coleção de palavras em A. Lembre que A^* denota o conjunto de todas as palavras de A. Logo, a linguagem L é apenas um subconjunto de A^*.

Exemplo 12.1 Seja $A = \{a, b\}$. Os itens a seguir são linguagens sobre A.

(a) $L_1 = \{a, ab, ab^2, \ldots\}$ (c) $L_3 = \{a^mb^m \mid m > 0\}$

(b) $L_2 = \{a^mb^n \mid m > 0, n > 0\}$ (d) $L_4 = \{b^mab^n \mid m > 0, n > 0\}$

É possível descrever verbalmente essas linguagens como se segue.

(a) L_1 consiste em todas as palavras que começam com a e são seguidas por zero ou mais b's.

(b) L_2 consiste em todas as palavras que começam com um ou mais a's e são seguidas por um ou mais b's.

(c) L_3 consiste em todas as palavras que começam com um ou mais a's e são seguidas pelo mesmo número de b's.

(d) L_4 consiste em todas as palavras com exatamente um a.

Operações sobre linguagens

Suponha que L e M são linguagens sobre um alfabeto A. Então a "concatenação" de L e M, denotada por LM, é a linguagem definida como se segue:

$$LM = \{uv \mid u \in L, v \in V\}$$

Isto é, LM denota o conjunto de todas as palavras que surgem da concatenação de uma palavra de L com uma palavra de M. Por exemplo, suponha que

$$L_1 = \{a, b^2\}, L_2 = \{a^2, ab, b^3\}, L_3 = \{a^2, a^4, a^6, \ldots\}$$

Então:

$$L_1 L_1 = \{a^2, ab^2, b^2a, b^4\}, L_1 L_2 = \{a^3, a^2b, ab^3, b^2a^2, b^2ab, b^5\}$$
$$L_1 L_3 = \{a^3, a^5, a^7, \ldots, b^2a^2, b^2a^4, b^2a^6, \ldots\}$$

Claramente, a concatenação de linguagens é associativa, uma vez que a concatenação de palavras é associativa.

Potências de uma linguagem L são definidas como se segue:

$$L^0 = \{\lambda\}, L^1 = L, L^2 = LL, L^{m+1} = L^m L \text{ para } m > 1.$$

A operação monádica L^* (lê-se "L estrela") de uma linguagem L, chamada de fechamento *Kleene* de L, pois Kleene demonstrou o Teorema 12.2, é definida como uma união infinita

$$L^* = L^0 \cup L^1 \cup L^2 \cup \cdots = \bigcup_{k=0}^{\infty} L^k$$

A definição de L^* é compatível com a notação A^*, que consiste em todas as palavras sobre A. Alguns textos definem L^+ como sendo a união de $L^1, L^2, \ldots$, isto é, L^+ é o mesmo que L^*, mas sem a palavra vazia λ.

12.4 EXPRESSÕES REGULARES, LINGUAGENS REGULARES

Seja A um alfabeto (não vazio). Esta seção define uma expressão regular r sobre A e uma linguagem $L(r)$ sobre A associada com a expressão regular r. A expressão r e sua linguagem correspondente $L(r)$ são definidas intuitivamente como se segue:

Definição 12.1: Cada um dos itens a seguir é uma expressão regular sobre um alfabeto A.

(1) O símbolo "λ" (palavra vazia) e o par "( )" (expressão vazia) são expressões regulares.
(2) Cada letra a em A é uma expressão regular.
(3) Se r é uma expressão regular, então (r^*) é uma expressão regular.
(4) Se r_1 e r_2 são expressões regulares, então $(r_1 \vee r_2)$ é uma expressão regular.
(5) Se r_1 e r_2 são expressões regulares, então $(r_1 r_2)$ é uma expressão regular.

Todas as expressões regulares são formadas dessa maneira.

Observe que uma expressão regular r é um tipo especial de palavra (string) que usa as letras de A e os cinco símbolos.

$$(\quad) \quad * \quad \vee \quad \lambda$$

Enfatizamos que nenhum outro símbolo é usado para expressões regulares.

Definição 12.2: A linguagem $L(r)$ sobre A definida por uma expressão regular r sobre A é como se segue.

(1) $L(\lambda) = \{\lambda\}$ e $L(( )) = \varnothing$, o conjunto vazio.
(2) $L(a) = \{a\}$, onde a é uma letra em A.
(3) $L(r^*) = (L(r))^*$ (o fechamento de Kleene de $L(r)$).
(4) $L(r_1 \vee r_2) = L(r_1) \cup L(r_2)$ (a união das linguagens).
(5) $L(r_1 r_2) = L(r_1) L(r_2)$ (a concatenação das linguagens).

Observação: Parênteses são omitidos de expressões regulares sempre que possível. Uma vez que a concatenação e a união de linguagens são associativas, muitos dos parênteses podem ser omitidos. Além disso, adotando a convenção de que "*" tem precedência sobre a concatenação, e concatenação tem precedência sobre "$\vee$", outros parênteses podem ser omitidos.

Definição 12.3: Seja L uma linguagem sobre A. Então L é chamada de *linguagem regular* sobre A se existir uma expressão regular r sobre A tal que $L = L(r)$.

Exemplo 12.2 Seja $A = \{a, b\}$. Cada um dos itens a seguir é uma expressão r e sua linguagem $L(r)$ correspondente;

(a) Seja $r = a^*$. Então $L(r)$ consiste em todas as potências de a, incluindo a palavra vazia λ.

(b) Seja $r = aa^*$. Então $L(r)$ consiste em todas as potências positivas de a, excluindo a palavra vazia.

(c) Seja $r = a \vee b^*$. Então $L(r)$ consiste em a ou em qualquer palavra em b, isto é, $L(r) = \{a, \lambda, b, b^2, \cdots\}$.

(d) Seja $r = (a \vee b)^*$. Note que $L(a \vee b) = \{a\} \cup \{b\} = A$; logo, $L(r) = A^*$, todas as palavras sobre A.

(e) Seja $r = (a \vee b)^*bb$. Então $L(r)$ consiste na concatenação de qualquer palavra em A com bb, isto é, todas as palavras que terminem em b^2.

(f) Seja $r = a \wedge b^*$. $L(r)$ não existe, uma vez que r não é uma expressão regular. (Especificamente, $\wedge$ não é um dos símbolos usados para expressões regulares.)

Exemplo 12.3 Considere as seguintes linguagens sobre $A = \{a, b\}$:

(a) $L_1 = \{a^m b^n \mid m > 0, n > 0\}$; (b) $L_2 = \{b^m a b^n \mid m > 0, n > 0\}$; (c) $L_3 = \{a^m b^m \mid m > 0\}$.

Encontre uma expressão regular r sobre $A = \{a, b\}$ tal que $L_i = L(r)$ para $i = 1, 2, 3$.

(a) L_1 consiste nas palavras começando com um ou mais a's, seguidos de um ou mais b's. Logo, podemos fixar $r = aa^*bb^*$. Note que r não é único; por exemplo, $r = a^*abb^*$ é outra solução.

(b) L_2 consiste em todas as palavras que começam com um ou mais b's seguidos por apenas um a que é, então, seguido por um ou mais b's, isto é, todas as palavras com exatamente um a que não é nem a primeira, nem a última letra. Logo, $r = bb^*abb^*$ é uma solução.

(c) L_3 consiste em todas as palavras começando com um ou mais a's seguidos pelo mesmo número de b's. Não existe nenhuma expressão regular r tal que $L_3 = L(r)$; isto é, L_3 não é uma linguagem regular. A prova desse fato aparece no Exemplo 12.8.

12.5 AUTÔMATOS DE ESTADOS FINITOS

Um *autômato de estado finito* (AEF) ou, simplesmente, um *autômato M*, consiste em cinco componentes:

(1) Um conjunto finito (alfabeto) A de entradas (*inputs*).

(2) Um conjunto finito S de estados (internos).

(3) Um subconjunto Y de S (chamado de estados de aceitação ou de "sim").

(4) Um estado inicial s_0 em S.

(5) Uma função de próximo estado F de $S \times A$ em S.

Tal autômato M é denotado por $M = (A, S, Y, s_0, F)$ quando queremos indicar suas cinco componentes.

Alguns livros definem a função de próximo estado $F: S \times A \to S$ em (5) por meio de uma coleção de funções $f_a: S \to S$, para cada $a \in A$. Fazendo $F(s, a) = f_a(s)$ temos que ambas as definições são equivalentes.

Exemplo 12.4 Os itens a seguir definem um autômato M com dois símbolos de entrada e três estados.

(1) $A = \{a, b\}$, símbolos de entrada.

(2) $S = \{s_0, s_1, s_2\}$, estados internos.

(3) $Y = \{s_0, s_1\}$, estados "sim".

(4) s_0, estado inicial.

(5) Função de próximo estado $F : S \times A \to S$, definida explicitamente na Fig. 12-1(a) ou pela tabela na Fig. 12-1(b).

$F(s_0, a) = s_0, \; F(s_1, a) = s_0, \; F(s_2, a) = s_2$
$F(s_0, b) = s_1, \; F(s_1, b) = s_2, \; F(s_2, b) = s_2$

(a)

F	a	b
s_0	s_0	s_1
s_1	s_0	s_2
s_2	s_2	s_2

(b)

Figura 12-1

Diagrama de estados de um autômato *M*

Um autômato M é normalmente definido por meio de seu diagrama de estados $D = D(M)$ em vez de se listar suas cinco componentes. O diagrama de estados $D = D(M)$ é um grafo orientado rotulado como se segue.

(1) Os vértices de $D(M)$ são os estados em S e um estado de aceitação é denotado por um círculo duplo.

(2) Existe uma flecha (aresta orientada) em $D(M)$ do estado s_j ao estado s_k, rotulado por uma entrada a se $F(s_j, a) = s_k$ ou, de maneira equivalente, se $f_a(s_j) = s_k$.

(3) O estado inicial s_0 é indicado por meio de uma flecha especial que termina em s_0, mas não possui vértice inicial.

Para cada vértice s_j e cada letra a no alfabeto A, existe uma flecha partindo de s_j que é rotulada por a; logo, o grau de saída de cada vértice é igual ao número de elementos em A. Por questão de conveniência notacional, rotulamos uma única flecha para todas as entradas que causam a mesma mudança no estado em vez de ter uma flecha para cada uma dessas entradas.

O diagrama de estados $D = D(M)$ do autômato M no Exemplo 12.4 aparece na Fig. 12-2. Note que tanto a quanto b rotulam a flecha de s_2 a s_2, uma vez que $F(s_2, a) = s_2$ e $F(s_2, b) = s_2$. Observe também que o grau de saída de cada vértice é 2, o número de elementos em A.

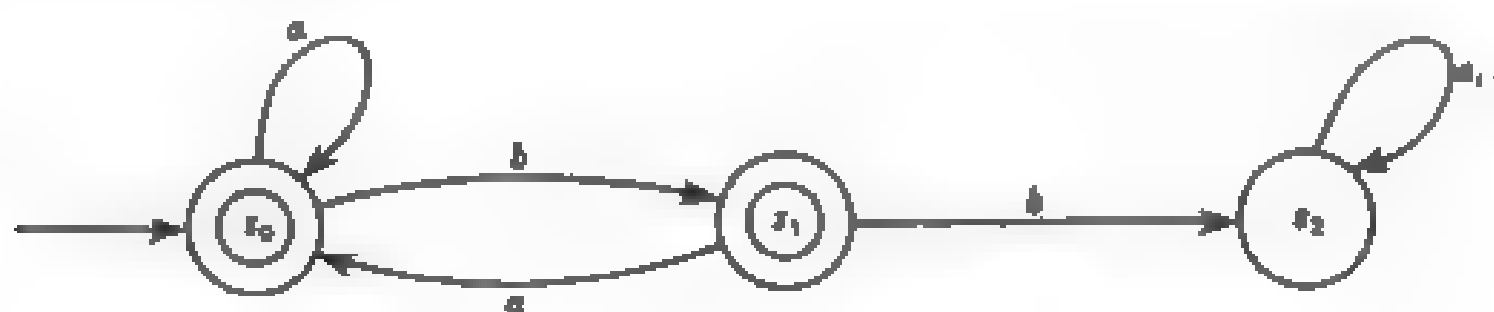



Figura 12-2

Linguagem *L(M)* determinada por um autômato *M*

Cada autômato M com um alfabeto de entrada A define uma linguagem sobre A, denotada por $L(M)$, como se segue.

Seja $w = a_1 a_2 \cdots a_m$ uma palavra em A. Então w determina o seguinte caminho no grafo do diagrama de estados $D(M)$, onde s_0 é o estado inicial e $F(s_{i-1}, a_i) = s_i$ para $i \geq 1$:

$$P = (s_0, a_1, s_1, a_2, s_2, \cdots, a_m, s_m)$$

Dizemos que M *reconhece* a palavra w se o estado final s_m é um estado de aceitação em Y. A linguagem $L(M)$ de M é a coleção de todas as palavras de A que são aceitas por M.

Exemplo 12.5 Determine se o autômato M na Fig. 12-2 aceita as palavras:

$$w_1 = ababba; \qquad w_2 = baab; \qquad w_3 = \lambda \text{ a palavra vazia}$$

Use a Fig. 12-2 e as palavras w_1 e w_2 para obter os seguintes caminhos respectivos:

$$P_1 = s_0 \xrightarrow{a} s_0 \xrightarrow{b} s_1 \xrightarrow{a} s_0 \xrightarrow{b} s_1 \xrightarrow{b} s_2 \xrightarrow{a} s_2 \text{ e } P_2 = s_0 \xrightarrow{b} s_1 \xrightarrow{a} s_0 \xrightarrow{a} s_0 \xrightarrow{b} s_1$$

O estado final em P_1 é s_2 que não está em Y, logo, w_1 não é aceito por M. Por outro lado, o estado final P_2 é s_1, que está em Y; portanto, w_2 é aceito por M. O estado final determinado por w_3 é o estado inicial s_0, uma vez que $w_3 = \lambda$ é a palavra vazia. Então, w_3 é aceito por M, uma vez que $s_0 \in Y$.

Exemplo 12.6 Descreva a linguagem $L(M)$ do autômato M na Fig. 12-2.

$L(M)$ consiste em todas as palavras w em A que não possuem dois b's sucessivos. Isso é consequência dos fatos a seguir:

(1) Podemos incluir o estado s_2 se, e somente se, existem dois b's sucessivos.

(2) Nunca podemos excluir s_2.

(3) O estado s_2 é o único estado de rejeição (não aceitação).

A relação fundamental entre linguagens regulares e autômatos está no seguinte teorema (cuja demonstração está além do escopo deste livro).

Teorema 12.2 (Kleene): Uma linguagem L sobre um alfabeto A é regular se, e somente se, existe um autômato M de estado finito tal que $L = L(M)$.

A operação estrela L^* em uma linguagem L é, às vezes, chamada de fechamento de Kleene de L, uma vez que Kleene provou o resultado básico mostrado acima.

Exemplo 12.7 Seja $A = \{a, b\}$. Construa um autômato M de tal forma que ele aceite precisamente as palavras de A que terminam com dois b's.

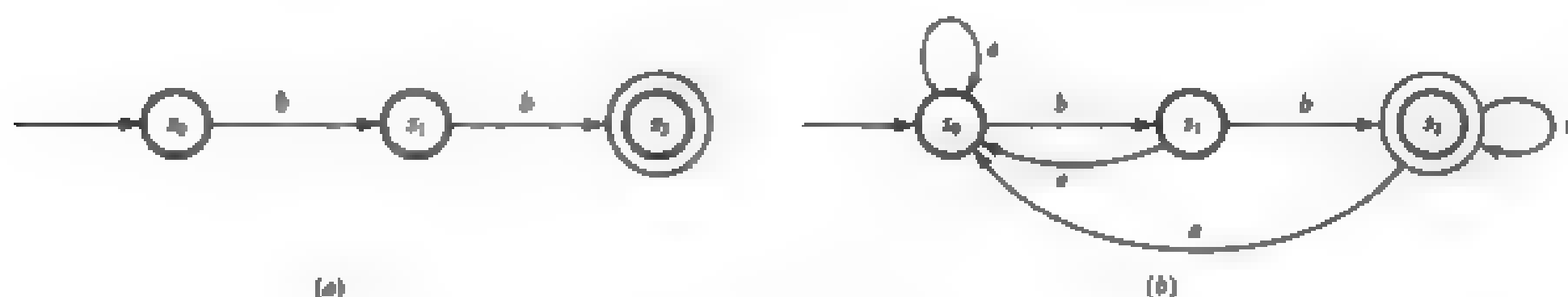



Figura 12-3

Uma vez que b^2 é aceito, mas não λ ou b, precisamos de três estados, s_0, o estado inicial, s_1 e s_2 com uma flecha rotulada por b que vai de s_0 a s_1 e outra que vai de s_1 a s_2. Além disso, s_2 é um estado de aceitação, enquanto s_0 e s_1 não são. Isso gera o grafo na Fig. 12-3(a). Por outro lado, se existe um a, então temos que voltar para s_0 e, se estamos em s_2 e existe um b, então ficamos em s_2. Essas condições adicionais nos dão o autômato M mostrado na Fig. 12-3(b).

Lema do bombeamento

Seja M um autômato sobre A com k estados. Suponha que $w = a_1a_2 \cdots a_n$ é uma palavra sobre A aceita por M, e suponha também que $|w| = n > k$, o número de estados. Seja

$$P = (s_0, s_1, \ldots, s_n)$$

a sequência correspondente de estados determinada pela palavra w. Uma vez que $n > k$, dois dos estados em P devem ser iguais. Consideremos $s_i = s_j$, onde $i < j$. Seja w dividido em subpalavras x, y e z como se segue:

$$x = a_1a_2 \cdots a_i, \quad y = a_{i+1} \cdots a_j, \quad z = a_{j+1} \cdots a_n$$

Como mostrado na Fig. 12-4, xy termina em $s_i = s_j$, uma vez que xy^m também termina em s_i. Logo, para todo m, $w_m = xy^m z$ termina em s_n, que é um estado de aceitação.

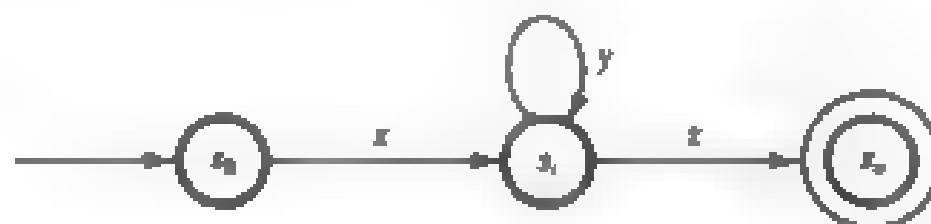



Figura 12-4

A discussão acima prova o resultado importante que se segue.

Teorema 12.3 (Lema do Bombeamento): Suponha que M seja um autômato sobre A de tal forma que:

(i) M possui k estados. (ii) M aceita uma palavra w de A onde $|w| > k$.

Então $w = xyz$, onde, para todo m positivo, $w_m = xy^m z$ é aceito por M.

O próximo exemplo mostra uma aplicação do Lema do Bombeamento.

Exemplo 12.8 Mostre que a linguagem $L = \{a^m b^m \mid m \text{ é positivo}\}$ não é regular.

Suponha que L é regular. Então, segundo o Teorema 12.2, existe um autômato M de estado finito que aceita L. Suponha que M tem k estados. Seja $w = a^k b^k$. Então $|w| > k$. Segundo o Lema do Bombeamento (Teorema 12.3), $w = xyz$, onde y não é vazio e $w_2 = xy^2 z$ também é aceito por M. Se y consiste apenas em a's e b's, então w^2 não tem o mesmo número de a's e b's. Se y contém tanto a's quanto b's, então w_2 tem b's seguidos de a's. Em qualquer um dos casos, w_2 não pertence a L, o que é uma contradição. Logo, L não é regular.

12.6 GRAMÁTICAS

A Figura 12-5 mostra a construção gramatical de uma sentença específica. Observe que existem:

(1) várias variáveis, por exemplo, ⟨sentença⟩, ⟨frase substantiva⟩, ⋯;

(2) várias palavras terminais, por exemplo, "O", "garoto", ⋯;

(3) uma variável inicial ⟨sentença⟩;

(4) várias substituições, ou produções, por exemplo,

$$\begin{aligned} \langle\text{sentença}\rangle &\rightarrow \langle\text{sintagma nominal}\rangle\ \langle\text{sintagma verbal}\rangle \\ \langle\text{objeto}\rangle &\rightarrow \langle\text{artigo}\rangle\ \langle\text{substantivo}\rangle \\ \langle\text{substantivo}\rangle &\rightarrow \text{maçã} \end{aligned}$$

A sentença final contém apenas terminais, apesar de tanto as variáveis quanto as terminais aparecerem em sua construção por meio das produções. Essa descrição intuitiva é dada com o objetivo de motivar a definição a seguir de uma gramática e a linguagem que ela gera.

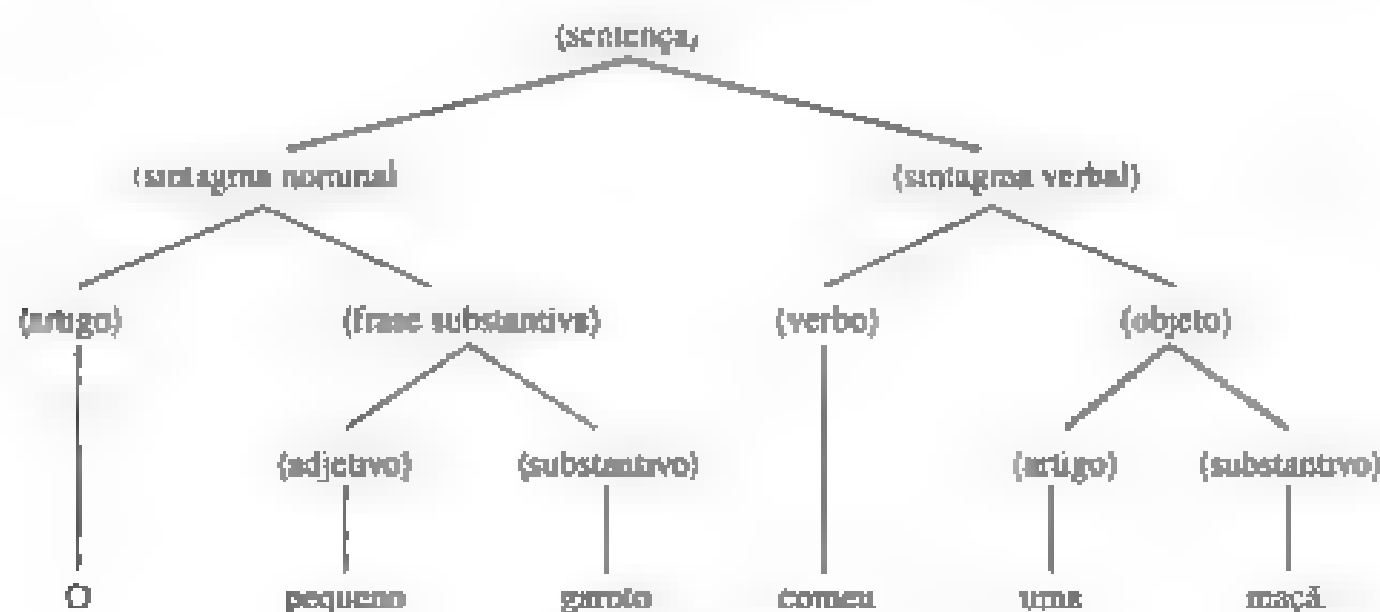



Figura 12-5

Definição 12.4: Uma *gramática de estrutura de frases* ou, simplesmente, uma *gramática G* consiste em quatro componentes.

(1) Um conjunto finito (vocabulário) V.

(2) Um subconjunto T de V, cujos elementos são chamados de *terminais*; os elementos de $N = V \setminus T$ são chamados de *não terminais* ou *variáveis*.

(3) Um símbolo S não terminal chamado de símbolo *inicial*.

(4) Um conjunto finito P de produções. (Uma produção é um par ordenado (α, β), normalmente escrito como $\alpha \to \beta$, onde α e β são palavras em V, e a produção deve conter pelo menos um elemento não terminal no seu lado esquerdo α.)

Tal gramática G é denotada por $G = G(V, T, S, P)$ quando queremos indicar suas quatro componentes.

A notação a seguir é usada para as nossas gramáticas, a menos que dito implícita ou explicitamente o contrário. Terminais são denotados com letras latinas minúsculas em itálico, $a, b, c, \cdots$, e não terminais são denotados pelas maiúsculas, $A, B, C, \cdots$, com S como o símbolo inicial. Do mesmo modo, letras gregas, $\alpha, \beta, \cdots$, denotam palavras em V, isto é, palavras em terminais e não terminais. Além disso, escrevemos

$$\alpha \to (\beta_1, \beta_2, \cdots, \beta_k) \text{ em vez de } \alpha \to \beta_1, \alpha \to \beta_2, \cdots, \alpha \to \beta_k$$

Observação: Frequentemente, definimos uma gramática G usando apenas suas produções, assumindo implicitamente que S é o símbolo inicial e os terminais e não terminais de G são apenas aqueles que aparecem nas produções.

Exemplo 12.9 A seguir, definimos uma gramática G com S como o símbolo inicial

$$V = \{A, B, S, a, b\}, T = \{a, b\}, P = \{S \xrightarrow{1} AB, A \xrightarrow{2} Aa, B \xrightarrow{3} Bb, A \xrightarrow{4} a, B \xrightarrow{5} b\}$$

A produção pode ser abreviada como se segue: $S \to AB, A \to (Aa, a), B \to (Bb, b)$

Linguagem $L(G)$ de uma gramática G

Suponha que w e w' são palavras sobre o conjunto V do vocabulário de uma gramática G. Escrevemos

$$w \Rightarrow w'$$

se w' pode ser obtida a partir de w, usando uma das produções, isto é, se existem palavras u e v tal que $w = u\alpha v$ e $w' = u\beta v$ e exista uma produção $\alpha \to \beta$. Além disso, escrevemos

$$w \Rightarrow\Rightarrow w' \text{ ou } w \overset{*}{\Rightarrow} w'$$

se w' pode ser obtida a partir de w, usando um número finito de produções.

Agora, seja G uma gramática com conjunto T terminal. A linguagem de G, denotada por $L(G)$, consiste em todas as palavras em T que possam ser obtidas a partir do símbolo inicial S ao se usar o processo acima; isto é,

$$L(G) = \{w \in T^* : S \Rightarrow\Rightarrow w\}$$

Exemplo 12.10 Considere a gramática G no Exemplo 12.9. Observe que $w = a^2b^4$ pode ser obtida a partir do símbolo inicial S como se segue:

$$S \Rightarrow AB \Rightarrow AaB \Rightarrow aaB \Rightarrow aaBb \Rightarrow aaBbb \Rightarrow aaBbbb \Rightarrow aabbbb = a^2b^4$$

Aqui usamos as produções 1, 2, 4, 3, 3, 3 e 5, respectivamente. Logo, podemos escrever $S \Rightarrow\Rightarrow a^2b^4$. Então $w = a^2b^4$ pertence a $L(G)$. De forma mais geral, a sequência de produções:

1, 2 (r vezes), 4, 3 (s vezes), 5

produzirá a palavra $w = a^r ab^s b$, onde r e s são inteiros não negativos. Por outro lado, não há sequência de produções que possam gerar um a depois de um b. Consequentemente,

$$L(G) = \{a^m b^n \quad m \text{ e } n \text{ são inteiros positivos}\}$$

Isto é, a linguagem $L(G)$ da gramática G consiste em todas as palavras que começam com um ou mais a's, seguidos de um ou mais b's.

Exemplo 12.11 Encontre a linguagem $L(G)$ sobre $\{a, b, c\}$ gerada pela gramática G:

$$S \to aSb, \quad aS \to Aa, \quad Aab \to c$$

Antes de mais nada, devemos aplicar a primeira produção uma ou mais vezes para obter a palavra $w = a^n Sb^n$, onde $n > 0$. Para eliminar S, devemos aplicar a segunda produção para obtermos a palavra $w' = a^m Aabb^m$, onde $m = n$ $1 \geq 0$. Agora, só podemos aplicar a terceira produção para finalmente obter a palavra $w'' = a^m cb^m$, onde $m \geq 0$. Consequentemente,

$$L(G) = \{a^m cb^m \mid m \text{ não negativo}\}$$

Isto é, $L(G)$ consiste em todas as palavras com o mesmo número não negativo de a's e b's, separados por a c.

Tipos de gramáticas

Gramáticas são classificadas de acordo com os tipos de produções que são permitidas. A classificação de gramáticas a seguir é devida a Noam Chomsky.

Uma gramática Tipo 0 não possui restrições em suas produções. Tipos 1, 2 e 3 são definidas como se segue:

(1) Uma gramática G é dita do Tipo 1 se toda produção é da forma $\alpha \to \beta$, onde $|\alpha| \leq |\beta|$, ou da forma $\alpha \to \lambda$.

(2) Uma gramática G é do Tipo 2 se toda produção é da forma $A \to \beta$, onde o lado esquerdo A é um elemento não terminal.

(3) Uma gramática G é do Tipo 3 se toda produção é da forma $A \to a$ ou $A \to aB$, isto é, onde o lado esquerdo A é um único elemento não terminal, e o lado direito é um único elemento terminal, ou um terminal seguindo por um não terminal, ou da forma $S \to \lambda$.

Observe que as gramáticas formam uma hierarquia, isto é, toda gramática do Tipo 3 é também do Tipo 2, assim como toda Tipo 2 é, também, uma Tipo 1, e, por sua vez, a Tipo 1 é do Tipo 0.

Gramáticas são também classificadas como sensíveis a contexto, livres de contexto e regulares, como se segue.

(a) Uma gramática G é *sensível a contexto* se as produções são da forma

$$\alpha A \alpha' \to \alpha \beta \alpha'$$

O nome "sensível a contexto" vem do fato de que podemos substituir a variável A por β em uma palavra apenas quando A está entre α e α'.

(b) Uma gramática G é dita *livre de contexto* se as produções são da forma

$$A \to \beta$$

O termo "livre de contexto" se origina do fato de que podemos, agora, substituir a variável A por β independentemente de onde A aparece.

(c) Uma gramática G é dita como *regular* se as produções são da forma

$$A \to a, \quad A \to aB, \quad S \to \lambda$$

Observe que uma gramática livre de contexto é o mesmo que uma gramática do Tipo 2, e uma gramática regular é do Tipo 3.

Segue uma relação fundamental entre gramáticas regulares e autômatos finitos

Teorema 12.4: Uma linguagem L pode ser gerada por uma gramática G do Tipo 3 (regular) se, e somente se, existir um autômato M finito que aceite L.

Logo, uma linguagem L é regular sss $L = L(r)$, onde r é uma expressão regular, sss $L = L(M)$, onde M é um autômato finito sss $L = L(G)$, sendo que G é uma gramática regular. (Lembre que (sss) é uma abreviação para "se, e somente se,".)

Exemplo 12.12 Considere a linguagem $L = \{a^n b^n \mid n > 0\}$.

(a) Encontre uma gramática G livre de contexto que gere L.

Claramente, a gramática G com as seguintes produções gera L:

$$S \to ab, S \to aSb$$

Note que G é livre de contexto.

(b) Encontre uma gramática G regular que gere L.

De acordo com o Exemplo 12.8, L não é uma linguagem regular. Logo, L não pode ser gerada por uma gramática regular.

Árvores de derivação de gramáticas livres de contexto

Considere uma gramática G livre de contexto (Tipo 2). Qualquer derivação de uma palavra w em $L(G)$ pode ser representada por meio de uma árvore ordenada enraizada T, chamada de *árvore de derivação*. Ilustramos tal árvore de derivação abaixo.

Seja G uma gramática livre de contexto com as produções a seguir:

$$S \to aAB, \quad A \to Bba, \quad B \to bB, \quad B \to c$$

A palavra $w = acbabc$ pode ser derivada de S como se segue:

$$S \Rightarrow aAB \Rightarrow a(Bba)B \Rightarrow acbaB \Rightarrow acba(bB) \Rightarrow acbabc$$

É possível desenhar uma árvore de derivação T da palavra w, como indicado pela Fig. 12-6. Especificamente, começamos com S como a raiz, e adicionamos ramos de acordo com a produção usada na derivação de w. Isso implica a árvore T completa que é mostrada na Fig. 12-6(e). A sequência de folhas da esquerda para a direita em T é a palavra derivada w. Além disso, qualquer elemento que não seja uma folha em T é uma variável, digamos, por exemplo, A, e os sucessores imediatos (filhos) de A, formam a palavra α, onde $A \to \alpha$ é a produção de G usada na derivação de w.

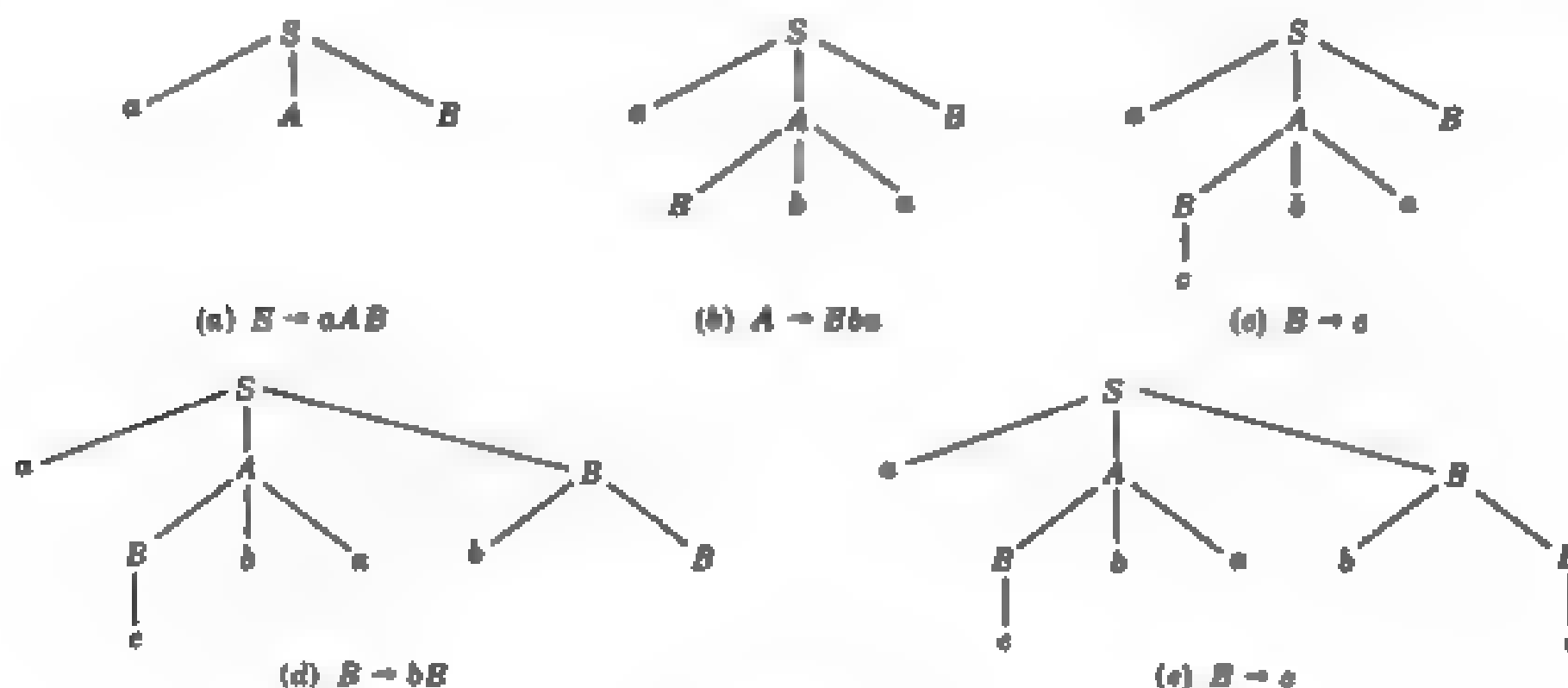



Figura 12-6

Forma de Backus-Naur

Existe outra notação, chamada de forma de Backus-Naur, que é usada ocasionalmente para se descrever as produções de uma gramática livre de contexto (Tipo 2). Especificamente:

(i) "::=" é usado em vez de "→."

(ii) Todo elemento não terminal é envolto entre parênteses ().

(iii) Todas as produções com o mesmo lado esquerdo não terminal são combinadas em uma sentença com todos os lados direitos listados à direita de ::=, separados por barras verticais.

Por exemplo, as produções $A \to aB$, $A \to b$, $A \to BC$ são combinadas em um único elemento:

$$(A) ::= a\ (B)\ |b|\ (B)\ (C)$$

Máquinas e gramáticas

O Teorema 12.4 estabelece que linguagens regulares correspondem ao autômato de estado finito (AEF). Existem também máquinas, mais potentes que o AEF, que correspondem às outras gramáticas.

(a) **Autômato pushdown:** Um autômato pushdown P é similar ao AEF, exceto pelo fato de que P possui uma pilha auxiliar que fornece uma quantia ilimitada de memória para P. Uma linguagem L é reconhecida por um autômato pushdown P se, e somente se, L for livre de contexto.

(b) **Autômato limitado Linear:** Um autômato limitado linear B é mais potente que o autômato pushdown. O autômato B faz uso de uma fita que é delimitada linearmente pelo comprimento da palavra de entrada w. Uma linguagem L é reconhecida por um autômato limitado linear B se, e somente se, L for sensível a contexto.

(c) **Máquina de Turing:** Uma máquina de Turing M, batizada com o nome do matemático britânico Alan Turing, usa uma fita infinita, ela é capaz de reconhecer qualquer linguagem L que possa ser gerada por qualquer estrutura gramatical de frases G. Na verdade, uma máquina de Turing M é apenas um dos vários meios equivalentes de se definir a noção de uma função "computável".

A discussão do autômato pushdown e do autômato limitado linear está além do escopo deste livro. Discutimos máquinas de Turing no Capítulo 13.

Problemas Resolvidos

Palavras

12.1 Considere as palavras $u = a^2ba^3b^2$ e $v = bab^2$. Encontre: (a) uv; $|uv|$, (b) vu; $|vu|$, (c) v^2, $|v^2|$.

Escreva as letras da primeira palavra seguidas pelas da segunda palavra, então conte o número total de letras na palavra resultante.

(a) $uv = (a^2ba^3b^2)(bab^2) = a^2ba^3b^3ab^2$; $|uv| = 12$

(b) $vu = (bab^2)(a^2ba^3b^2) = bab^2a^2ba^3b^2$, $|vu| = 12$

(c) $v^2 = vv = (bab^2)(bab^2) = bab^3ab^2$ $|v^2| = 8$

12.2 Suponha que $u = a^2b$ e $v = b^3ab$. Encontre: (a) uvu; (b) λu, $u\lambda$, $u\lambda v$.

(a) Escreva as letras em u, depois em v e, finalmente, em u para obter $uvu = a^2b^4aba^2b$.

(b) Uma vez que λ é a palavra vazia, $\lambda u = u\lambda = u = a^2b$ e $u\lambda v = uv = a^2b^4ab$.

12.3 Seja $w = abcd$. (a) Encontre todas as subpalavras de w. (b) Quais delas são segmentos iniciais?

(a) As subpalavras são: λ, a, b, c, d, ab, bc, cd, abc, bcd, $w = abcd$. (Enfatizamos que $v = acd$ não é uma subpalavra de w, mesmo considerando que todas as suas letras pertencem a w.)

(b) Os segmentos iniciais são λ, a, ab, abc, $w = abcd$.

12.4 Para quaisquer palavras u e v, mostre que: (*a*) $|uv| = |u| + |v|$; (b) $|uv| = |vu|$

(*a*) Suponha que $|u| = r$ e $|v| = s$. Então uv consiste nas r letras de u, seguidas pelas s letras de v, logo, $|uv| = r + s = |u| + |v|$

(*b*) Usar (*a*) implica $|uv| = |u| + |v| = |v| + |u| = |vu|$.

12.5 Descreva a diferença entre o semigrupo livre em um alfabeto A e o monoide livre em A.

O semigrupo livre em A é o conjunto de todas as palavras não vazias em A sob a operação de concatenação; isso não inclui a palavra vazia λ. Por outro lado, o monoide livre em A inclui a palavra vazia λ.

Linguagens

12.6 Seja $A = \{a, b\}$ Descreva verbalmente as seguintes linguagens sobre A (que são subconjuntos de A^*):

(*a*) $L_1 = \{(ab)^m \mid m > 0\}$; (*b*) $L_2 = \{a^r b a^s b a^t \mid r, s, t \geq 0\}$, (*c*) $L_3 = \{a^2 b^m a^3 \mid m > 0\}$

(*a*) L_1 consiste nas palavras $w = ababab \ldots ab$, isto é, começando com a, alternando com b, e terminando novamente com b.

(*b*) L_2 consiste em todas as palavras com exatamente dois b's.

(*c*) L_3 consiste em todas as palavras começando com a^2 e terminando com a^3, com um ou mais b's entre eles.

12.7 Sejam $K = \{a, ab, a^2\}$ e $L = \{b^2, aba\}$ linguagens sobre $A = \{a, b\}$ Encontre: (*a*) $K L$, (*b*) $L L$.

(*a*) Concatene palavras em K com palavras em L para obter $KL = \{ab^2, a^2ba, ab^3, ababa, a^2b^2, a^3ba\}$

(*b*) Concatene palavras em L com palavras em L para obter $LL = \{b^4, b^2aba, abab^2, aba^2ba\}$

12.8 Considere a linguagem $L = \{ab, c\}$ sobre $A = \{a, b, c\}$ Encontre: (*a*) L^0; (*b*) L^3; (*c*) L^{-2}

(*a*) $L^0 = \{\lambda\}$, por definição.

(*b*) Forme todas as sequências de três palavras a partir de L para obter:

$$L^3 = \{ababab, ababc, abcab, abc^2, cabab, cabc, c^2ab, c^3\}$$

(*c*) A potência negativa de uma linguagem não é definida.

12.9 Seja $A = \{a, b, c\}$. Encontre L^* onde: (*a*) $L = \{b^2\}$; (*b*) $L = \{a, b\}$, (*c*) $L = \{a, b, c^3\}$.

(*a*) L^* consiste em todas as palavras b^n onde n é par (incluindo a palavra vazia λ).

(*b*) L^* consiste em todas as palavras em a e b.

(*c*) L^* consiste em todas as palavras de A com a propriedade de que o comprimento de cada subpalavra maximal composta inteiramente por c's é divisível por 3.

12.10 Considere um alfabeto contável $A = \{a_1, a_2, \ldots\}$. Seja L_k a linguagem sobre A que consiste nas palavras w, tal que a soma dos subscritos das letras em w seja igual a k. (Por exemplo, $w = a_2a_3a_3a_6a_4$ pertence a L_{18}.) (*a*) Encontre L_4. (*b*) Mostre que L_k é finito. (*c*) Mostre que A^* é contável. (*c*) Mostre que qualquer linguagem sobre A é contável

(*a*) Nenhuma palavra em L_4 pode ter mais de quatro letras, e nenhuma letra a_n com $n > 4$ pode ser usada.

Logo, obtemos a seguinte lista:

$$a_1a_1a_1a_1,\quad a_1a_1a_2,\quad a_1a_2a_1,\quad a_2a_1a_1,\quad a_1a_3,\quad a_3a_1,\quad a_2a_2,\quad a_4$$

(*b*) Apenas um número finito dos a's, isto é, $a_1, a_2, \ldots, a_k$, pode ser usado em L_k, e nenhuma palavra em L_k pode ter mais de k letras. Logo, L_k é finito.

(*c*) A^* é a união contável dos conjuntos finitos L_k; logo, A^* é contável.

(*d*) L é um subconjunto do conjunto contável A^*; logo, L é contável também.

Expressões e linguagens regulares

12.11 Seja $A = \{a, b\}$. Descreva a linguagem $L(r)$ onde:

(a) $r = abb^*a$; (b) $r = b^*ab^*ab^*$; (c) $r = a^* \vee b^*$; (d) $r = ab^* \wedge a^*$.

(a) $L(r)$ consiste em todas as palavras que começam e terminam em a e que contêm um ou mais b's.

(b) $L(r)$ consiste em todas as palavras com exatamente dois a's.

(c) $L(r)$ consiste em todas as palavras apenas em a, ou apenas em b, isto é, $L(r) = \{\lambda, a, a^2, \ldots, b, b^2, \ldots\}$

(d) Aqui r não é uma expressão regular, uma vez que $\wedge$ não é um dos símbolos usados na formação de expressões regulares.

12.12 Sejam $A = \{a, b, c\}$ e $w = abc$. Descubra se w pertence ou não a $L(r)$, onde:

(a) $r = a^* \vee (b \vee c)^*$; ($b$) $r = a^* (b \vee c)^*$

(a) Não. Aqui $L(r)$ consiste em palavra em a, ou de palavras em b e c.

(b) Sim, uma vez que $a \in L(a)^*$ e $bc \in (b \vee c)^*$.

12.13 Seja $A = \{a, b\}$. Encontre uma expressão regular r tal que $L(r)$ consista em todas as palavras w, onde:

(a) w comece com a^2 e termine com b^2; (b) w contenha um número par de a's.

(a) Seja $r = a^2(a \vee b)^*b^2$. (Note que $(a \vee b)^*$ consiste em todas as palavras em A.)

(b) Note que $s = b^*ab^*ab^*$ consiste em todas as palavras com exatamente dois a's. Então, considere que $r = s^* = (b^*ab^*ab^*)^*$

Autômatos finitos

12.14 Seja M o autômato com o seguinte conjunto de entradas A, o conjunto de estado S com estado inicial s_0 e o conjunto de estado de aceitação ("sim") Y:

$$A = \{a, b\}, S = \{s_0, s_1, s_2\}, Y = \{s_2\}$$

Suponha que a função de próximo estado F de M é dada pela tabela da Fig. 12-7(a).

(a) Esboce o diagrama de estados $D = D(M)$ de M.

(b) Descreva a linguagem $L = L(M)$ aceita por M.

(a) O diagrama de estados D aparece na Fig. 12-7(b). Os vértices de D são os estados, e um círculo duplo indica um estado de aceitação. Se $F(s_j, x) = s_k$, então existe uma aresta orientada de s_j a s_k, rotulada pelo símbolo de entrada x. Além disso, existe uma flecha especial que termina no estado inicial s_0.

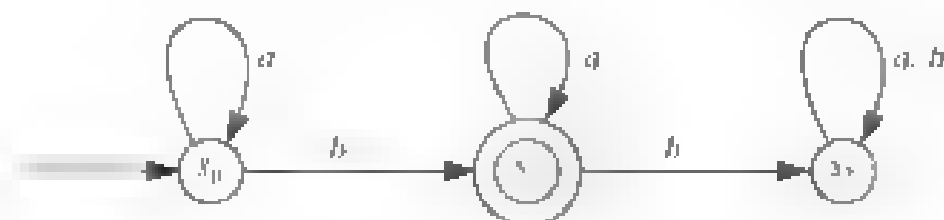
(b) $L(M)$ consiste em todas as palavras w com exatamente um b. Especificamente, se uma palavra de entrada w não possui b's, então ela termina em s_0, e se w possui dois ou mais b's, então ela termina em s_2. Caso contrário, w termina em s_1, que é o único estado de aceitação.

(a) (b)

Figura 12-7

12.15 Seja $A = \{a, b\}$. Construa um autômato M que aceita precisamente as palavras de A que possuem um número par de a's. Por exemplo, $aababbab$, aa, bbb, $ababaa$ são aceitas por M, mas $ababa$, aaa, $bbabb$ são rejeitadas.

Precisamos de apenas dois estados, s_0 e s_1. Assumimos que M está no estado s_0 ou s_1, dependendo se o número de a's, a menos do passo dado, é par ou ímpar. (Logo, s_0 é um estado de aceitação, mas s_1 é um estado de rejeição.) Então, apenas a muda o estado. Além disso, s_0 é o estado inicial.

O diagrama de estados de M é mostrado na Fig. 12-8(a).

12.16 Seja $A = \{a, b\}$. Construa um autômato M que aceita as palavras de A que comecem com a seguido por (zero ou mais) b's.

O autômato M aparece na Fig. 12-8(b).

Figura 12-8

12.17 Descreva as palavras w na linguagem L que são aceitas pelo autômato M na Fig. 12-9(a).

O sistema pode chegar ao estado de aceitação s_2 apenas quando existir a em w que segue um b.

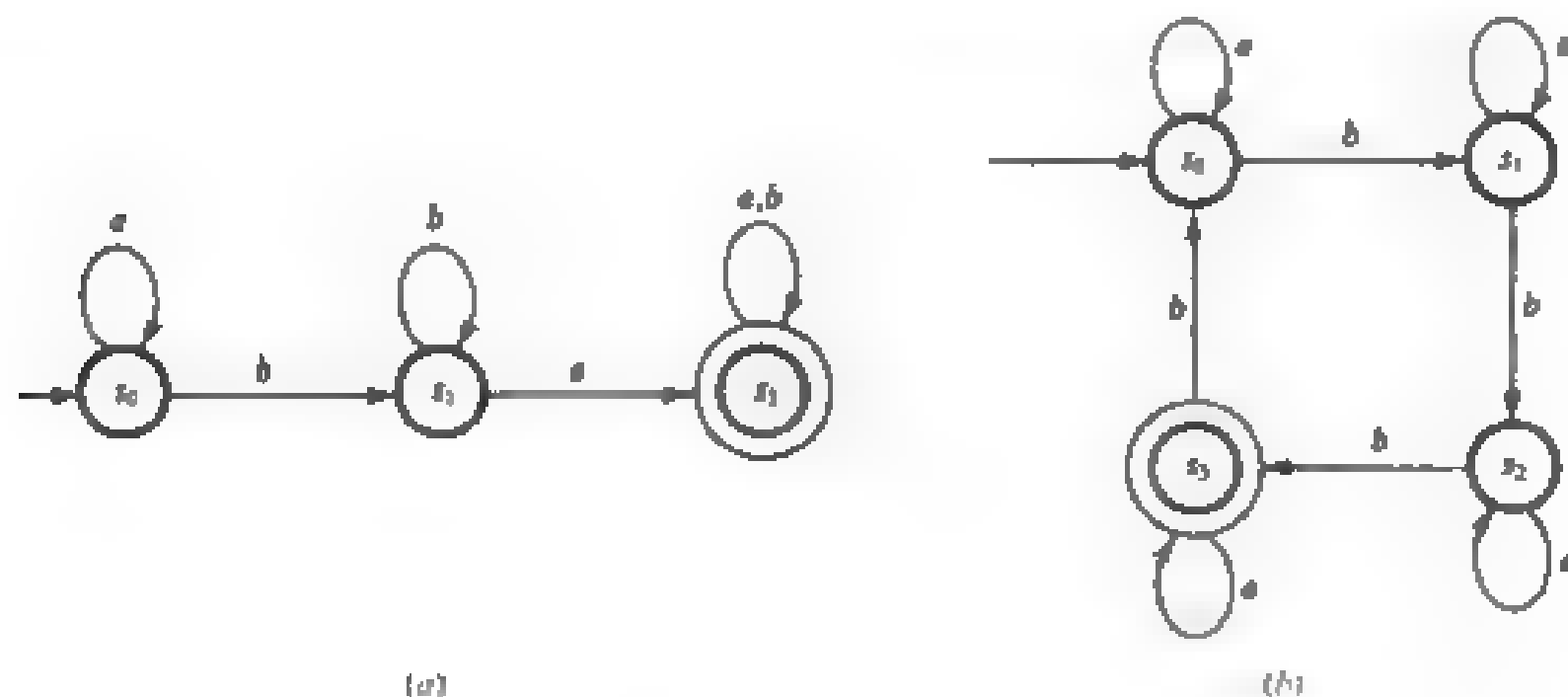



Figura 12-9

12.18 Descreva as palavras w na linguagem L aceitas pelo autômato M na Fig. 12-9(b).

Cada a em w não muda o estado do sistema, mas cada b em w muda o estado de R para s_{i+1} (módulo 4). Logo, w é aceito por M se o número n de b's em w for congruente a 3 módulo 4, isto é, onde $n = 3, 7, 11, \ldots$

12.19 Suponha que L é uma linguagem sobre A que é aceita pelo autômato $M = (A, S, Y, s_0, F)$. Encontre um autômato N que aceite L^C, isto é, as palavras de A que não pertencem a L.

Apenas permute os estados de aceitação e rejeição em M para obter N. Então w é aceito na nova máquina N se, e somente se, w for rejeitado em M, isto é, se, e somente se, w pertencer a L^C. Formalmente, $N = (A, S, S\backslash Y, s_0, F)$.

12.20 Sejam $M = (A, S, Y, s_0, F)$ e $M' = (A, S', Y', S_0', F')$ autômatos sobre o mesmo alfabeto A que aceite as linguagens $L(M)$ e $L(M')$ sobre A, respectivamente. Construa um autômato N sobre A que aceite precisamente $L(M) \cap L(M')$.

Seja $S \times S'$ o conjunto de estados de N. Seja (s, s') um estado de aceitação de N se, tanto s quanto s' são estados de aceitação em M e M', respectivamente. Seja (s_0, s_0') o estado inicial de N. Considere a função de próximo estado de N, $G : (S \times S') \times A \rightarrow (S \times S')$, definida por

$$G((s, s'), a) = (F(s, a), F'(s', a))$$

Então N aceita precisamente as palavras em $L(M) \cap L(M')$.

12.21 Repita o Problema 12.20, mas agora considere N como aceitando precisamente $L(M) \cup L(M')$.

Novamente, sejam $S \times S'$ o conjunto de estados de N e (s_0, s_0) o estado inicial de N. Agora, considere $(S \times Y') \cup (Y \times S')$ como os estados de aceitação em N. A função de próximo estado G é, novamente, definida por

$$G((s, s'), a) = (F(s, a), F'(s', a))$$

Então N aceita precisamente as palavras em $L(M) \cup L(M')$.

Gramáticas

12.22 Defina: (*a*) gramática livre de contexto; (*b*) gramática regular.

(*a*) Uma gramática livre de contexto é o mesmo que uma gramática do Tipo 2, isto é, toda produção é da forma $A \to \beta$. Ou seja, o lado esquerdo é uma única variável, e o lado direito é uma palavra com um ou mais símbolos.

(*b*) Uma gramática regular é o mesmo que uma gramática do Tipo 3, isto é, toda produção é da forma $A \to a$ ou $A \to aB$, ou seja, o lado esquerdo é uma única variável, e o lado direito é um único terminal ou um terminal seguido de uma variável.

12.23 Encontre a linguagem $L(G)$ gerada pela gramática G com variáveis S, A, B, terminais a, b, e produções $S \to aB$, $B \to b$, $B \to bA$, $A \to aB$.

Observe que podemos usar a primeira produção somente uma vez, já que o símbolo inicial S não aparece em nenhum outro lugar. Além disso, podemos obter uma palavra terminal apenas ao usarmos a segunda produção. Caso contrário, adicionamos alternadamente a's e b's usando a terceira e a quarta produção. Consequentemente,

$$L(G) = \{(ab)^n = ababab \cdots ab \mid n \in N\}$$

12.24 Seja L a linguagem em $A = \{a, b\}$ que consiste em todas as palavras com exatamente um b, isto é,

$$L = \{b, a^r b, ba^s, a^r ba^s \mid r > 0, s > 0\}$$

(*a*) Encontre uma expressão regular r tal que $L = L(r)$.

(*b*) Encontre uma gramática regular G que gere a linguagem L.

(*a*) Seja $r = a^*ba^*$. Então $L(r) = L$.

(*b*) A gramática regular G, com as seguintes produções, gera L.

$$S \to (b, aA), \quad A \to (b, aA, bB), \quad B \to (a, aB)$$

Ou seja, a letra b só pode aparecer uma vez em qualquer palavra derivada de S. G é regular, já que ela possui a forma necessária para tal.

12.25 Seja G uma gramática regular com produções: $S \to aA$, $A \to aB$, $B \to bB$, $B \to A$.

(*a*) Encontre a árvore de derivação da palavra $w = aaba$.

(*b*) Descreva todas as palavras w na linguagem L gerada por G.

(*a*) Note, em primeiro lugar, que w pode ser derivada de S como se segue:

$$S \Rightarrow aA \Rightarrow a(aB) \Rightarrow aa(bB) \Rightarrow aaba$$

A Figura 12-10(*a*) mostra a árvore de derivação correspondente.

(*b*) Ao usar a produção 1, depois a 2 e então a 3 r vezes, e finalmente 4, derivamos a palavra $w = aab^r$, onde $r > 0$. Nenhuma outra palavra pode ser derivada de S.

12.26 A Figura 12-10(b) é a árvore de derivação de uma palavra w na linguagem L de uma gramática livre de contexto G. (a) Encontre w. (b) Quais terminais, variáveis e produções precisam estar em G?

(a) A sequência de folhas da esquerda para a direita implica a palavra $w = ababbbba$.

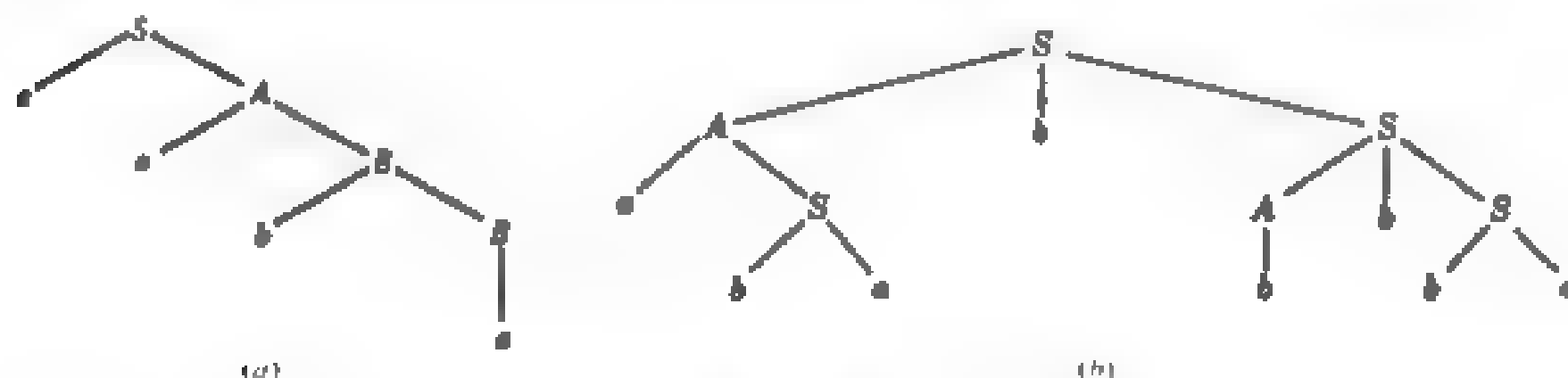



Figura 12-10

(b) As folhas mostram que a e b devem ser terminais, e os vértices internos mostram que S e A devem ser variáveis com S como variável inicial. Os filhos de cada variável mostram que $S \to AbS$, $A \to aS$, $S \to ba$ e $A \to b$ devem ser produções.

12.27 Uma árvore de derivação existe para qualquer palavra w derivada do símbolo S em uma gramática G?

Não. Árvores de derivação existem apenas para gramáticas dos Tipos 2 e 3, isto é, para gramáticas livres de contexto e regulares.

12.28 Determine o tipo de gramática G que consiste nas produções a seguir:

(a) $S \to aA$, $A \to aAB$, $B \to b$, $A \to a$

(b) $S \to aAB$, $AB \to bB$, $B \to b$, $A \to aB$

(c) $S \to aAB$, $AB \to a$, $A \to b$, $B \to AB$

(d) $S \to aB$, $B \to bA$, $B \to b$, $B \to a$, $A \to aB$, $A \to a$

(a) Cada produção é da forma $A \to \alpha$; logo, G é uma gramática livre de contexto ou de Tipo 2.

(b) O comprimento do lado esquerdo de cada produção não excede o comprimento do lado direito; logo, G é uma gramática do Tipo 1.

(c) A produção $AB \to a$ significa que G é uma gramática do Tipo 0.

(d) G é uma gramática regular ou do Tipo 3, uma vez que cada produção possui a forma $A \to a$ ou $A \to aB$.

12.29 Reescreva cada gramática G no Problema 12.28 na forma de Backus-Naur.

A forma de Backus-Naur apenas se aplica a gramáticas livre de contexto (o que inclui gramáticas regulares). Então, apenas (a) e (d) podem ser escritas nessa forma. A forma é obtida como se segue.

(i) Substitua $\to$ por $::=$.

(ii) Coloque não terminais entre parênteses $\langle\rangle$.

(iii) Todas as produções com o mesmo lado esquerdo são combinadas em uma única sentença com todos os lados direitos listados à direita de $::=$, separados por barras verticais.

Logo

(a) $\langle S\rangle ::= a\langle A\rangle$, $\langle A\rangle ::= a\langle A\rangle\langle B\rangle \mid a$, $\langle B\rangle ::= b$

(b) $\langle S\rangle ::= a\langle B\rangle$, $\langle B\rangle ::= b\langle B\rangle \mid b \mid a$, $\langle A\rangle ::= a\langle B\rangle \mid a$

Problemas Complementares

Palavras

12.30 Considere as palavras $u = ab^2a^3$ e $v = aba^2b^2$. Encontre. (*a*) uv; (*b*) vu, (*c*) u^2, (*d*) λu; (*e*) $v\lambda u$.

12.31 Para as palavras $u = ab^2a^3$ e $v = aba^2b^2$, encontre: $|u|$, $|v|$, $|uv|$, $|vu|$ e $|v^2|$.

12.32 Seja $w = abcde$. (a) Encontre todas as subpalavras de w. (b) Quais delas são segmentos iniciais?

12.33 Suponha que $u = a_1a_2 \cdots a_r$ e a_k são distintas. Encontre o número n de subpalavras de u.

Linguagens

12.34 Sejam $L = \{a^2, ab\}$ e $K = \{a, ab, b^2\}$. Encontre. (a) LK (b) KL, (c) $L \vee K$; (d) $K \wedge L$.

12.35 Seja $L = \{a^2, ab\}$. Encontre: (a) L^0; (b) L^2; (c) L^3.

12.36 Seja $A = \{a, b, c\}$. Descreva L^* se: (a) $L = \{a^2\}$; (b) $L = \{a, b^2\}$; (c) $\{a, b^2, c^3\}$.

12.37 $(L^2)^* = (L^*)^2$? Se não, como elas são relacionadas?

12.38 Considere um alfabeto contável $A = \{a_1, a_2, \ldots\}$. Seja L_k a linguagem sobre A que consiste em todas as palavras w tal que a soma dos subscritos das letras em w seja igual a k. (Ver Problema 12.10.) Encontre: (*a*) L_3, (*b*) L_5.

Expressões e linguagens regulares

12.39 Seja $A = \{a, b, c\}$. Descreva a linguagem $L(r)$ para cada uma das expressões regulares a seguir:

(*a*) $r = ab^*c$; (*b*) $r = (ab \vee c)^*$; (*c*) $r = ab \vee c^*$.

12.40 Seja $A = \{a, b\}$. Encontre uma expressão regular r tal que $L(r)$ consista em todas as palavras w, onde:

(a) w contenha exatamente três a's.

(b) O número de a's seja divisível por 3

12.41 Sejam $A = \{a, b, c\}$ e $w = ac$. Explique se w pertence a $L(r)$ ou não, onde:

(a) $r = a^*bc^*$; (b) $r = a^*b^*c$; (c) $r = (ab \vee c)^*$

12.42 Sejam $A = \{a, b, c\}$ e $w = abc$. Explique se w pertence a $L(r)$ ou não, onde.

(a) $r = ab^*(bc)^*$; (b) $r = a^* \vee (b \vee c)^*$; (c) $r = a^*b(bc \vee c^2)^*$.

Autômatos finitos

12.43 Seja $A = \{a, b\}$. Construa um autômato M tal que $L(M)$ consiste nas palavras w, onde

(a) o número de b's é divisível por 3. (b) w começa com a e termina com b.

12.44 Seja $A = \{a, b\}$. Construa um autômato M que aceita a linguagem:

(a) $L(M) = \{b^r ab^s \mid r > 0, s > 0\}$; (b) $L(M) = \{a^r b^s \mid r > 0, s > 0\}$

12.45 Seja $A = \{a, b\}$. Construa um autômato M tal que $L(M)$ consiste nas palavras em que o número de a's é divisível por 2, e o número de b's é divisível por 3.

(*Sugestão*: Use os Problemas 12.15, 12.43(a) e 12.20.)

12.46 Encontre a linguagem $L(M)$ aceita pelo autômato M na Fig. 12-11.

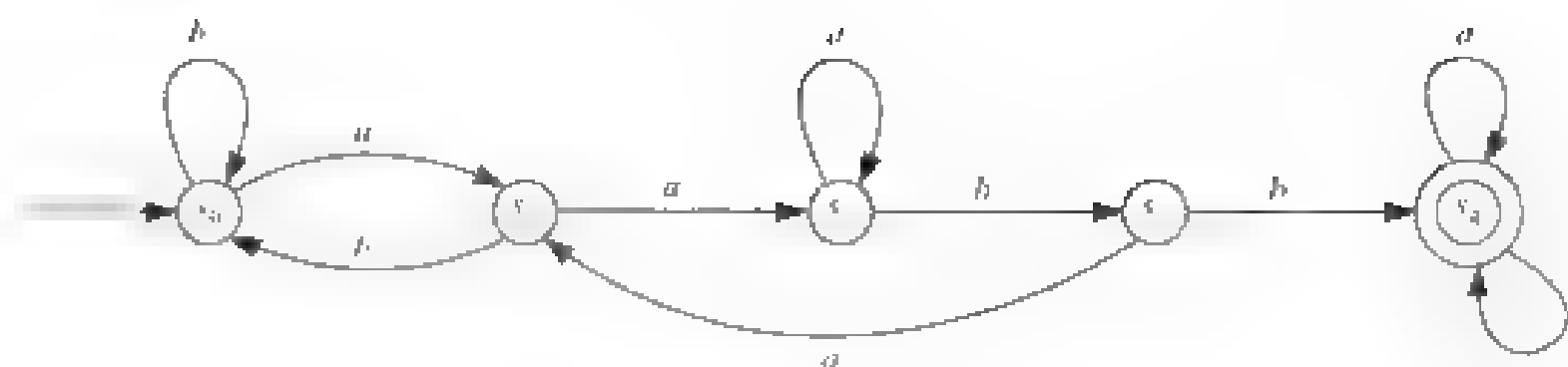



Figura 12-11

Gramáticas

12.47 Determine o Tipo de gramática G que consiste nas produções:

(a) $S \rightarrow aAB$, $S \rightarrow AB$; $A \rightarrow a$; $B \rightarrow b$

(b) $S \rightarrow aB$; $B \rightarrow AB$; $aA \rightarrow b$; $A \rightarrow a$; $B \rightarrow b$

(c) $S \rightarrow aB$; $B \rightarrow bB$; $B \rightarrow bA$; $A \rightarrow a$; $B \rightarrow b$

12.48 Encontre uma gramática regular G que gere a linguagem L que consista em todas as palavras em a e b tal que não existam dois a's em sequência.

12.49 Encontre uma gramática livre de contexto G que gere a linguagem L que consista em todas as palavras em a e em b em que o número de a's seja o dobro daquele de b's.

12.50 Encontre uma gramática G que gere a linguagem L que consista em todas as palavras em a e b com um número par de a's.

12.51 Encontre uma gramática G que gere a linguagem L que consista em todas as palavras da forma a^nba^n com $n > 0$

12.52 Mostre que a linguagem G no Problema 12.51 não é regular. (*Sugestão:* Use o Lema do Bombeamento.)

12.53 Descreva a linguagem $L = L(G)$ onde G tenha as produções $S \rightarrow aA$, $A \rightarrow bbA$, $A \rightarrow c$.

12.54 Descreva a linguagem $L = L(G)$ onde G tenha as produções $S \rightarrow aSb$, $Sb \rightarrow bA$, $abA \rightarrow c$.

12.55 Escreva cada gramática G do Problema 12.47 na forma de Backus-Naur.

12.56 Seja G uma gramática livre de contexto com as produções $S \rightarrow (a, aAS)$ e $A \rightarrow bS$.
(a) Escreva G na forma Backus-Naur. (b) Encontre a árvore de derivação da palavra $w = abaa$

12.57 A Figura 12-12 é a árvore de derivação de uma palavra w em uma linguagem L de uma gramática livre de contexto G
(a) Encontre w; (b) Quais terminais, variáveis e produções estão em G?

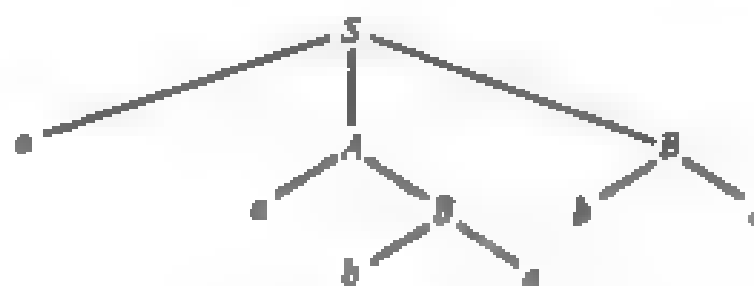



Figura 12-12

Respostas dos Problemas Complementares

12.30 (a) $uv = ab^2a^4ba^2b^2$, (b) $vu = aba^2b^2ab^2a^3$, (c) $u^2 = ab^2a^4b^2a^3$, (d) $\lambda u = u$, (e) $v\lambda v = v^2 = aba^2b^2aba^2b^2$

12.31 6, 6, 12, 12, 12.

12.32 (a) λ, a, b, c, d, e, ab, bc, cd, de, abc, bcd, cde, $abcd$, $bcde$, $w = abcde$.

(b) λ, a, ab, abc, $abcd$, $w = abcde$

12.33 Se $u = \lambda$, então $n = 1$; caso contrário, $n = 1 + [r + (r-1) + \cdots + 2 + 1] = 1 + r(r+1)/2$.

12.34 (a) $LK = \{a^3, a^3b, a^2b^2, aba, abab, ab^3\}$;

(b) $KL = \{a^3, a^2b, aba^2, abab, b^2a^2, b^2ab\}$,

(c) $L \vee K = \{a^2, ab, a, b^2\}$, (d) $K \wedge L$ não é definida

12.35 (a) $L^0 = \{\lambda\}$, (b) $L^2 = \{a^4, a^3b, aba^2, abab\}$, (c) $L^3 = \{a^6, a^5b, a^3ba^2, a^3bab, aba^4, aba^3b, ababa^2, ababab\}$

12.36 (a) $L* = \{a^n \mid n$ é par$\}$ (b) Todas as palavras w em a e b com apenas potências pares para b (c) Todas as palavras em a, b e c com cada potência de b sendo par, e cada potência de c sendo um múltiplo de 3.

12.37 Não. $(L^2)^* \subsetneq (L^*)^2$.

12.38 (a) $a_1a\ a$, a_1a_2, $a_2a_1a_3$ (b) $a \cdot a_1a_1a\ a_1$, $a\ a \cdot a_1a_3$, $a\ a \cdot a_2a_1$, $a_1a_2a\ a$, $a_2a_1a\ a$, $a_1a\ a_3$, $a\ a_2a_1$, a_2a_1a, a_2a_3, a_3a_2, a_1a_4, a_4a_1, a_5

12.39 (a) $L(r) = \{ab^nc \mid n \geq 0\}$ (b) Todas as palavras em x e c, onde $x = ab$. (c) $L(r) = ab \cup \{c^n \mid n \geq 0\}$

12.40 (a) $r = b^*ab^*ab^*ab^*$; (b) $r = (b^*ab^*ab^*ab^*)^*$

12.41 (a) Não; (b) sim, (c) não.

12.42 (a) Sim; (b) não; (c) não.

12.43 Ver: (a) Fig. 12-13(a); (b) Fig. 12-13(b).

12.44 Ver: (a) Fig. 12-14, (b) Fig. 12-15(a).

12.45 Ver: Fig. 12-15(b).

12.46 $L(M)$ consiste em todas as palavras w que contêm $aabb$ como uma subpalavra.

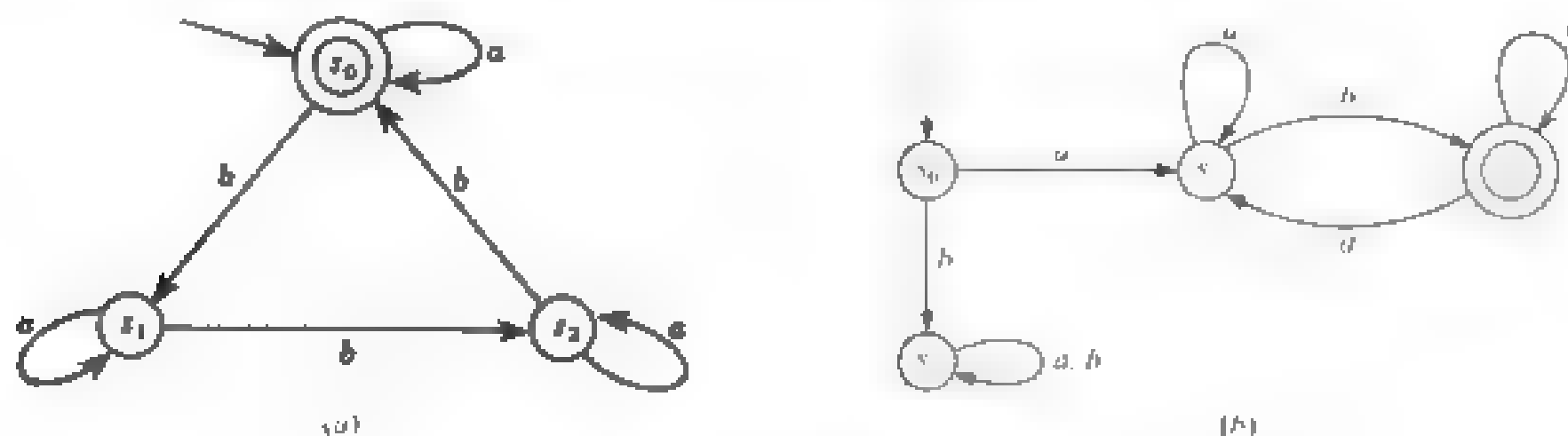



Figura 12-13

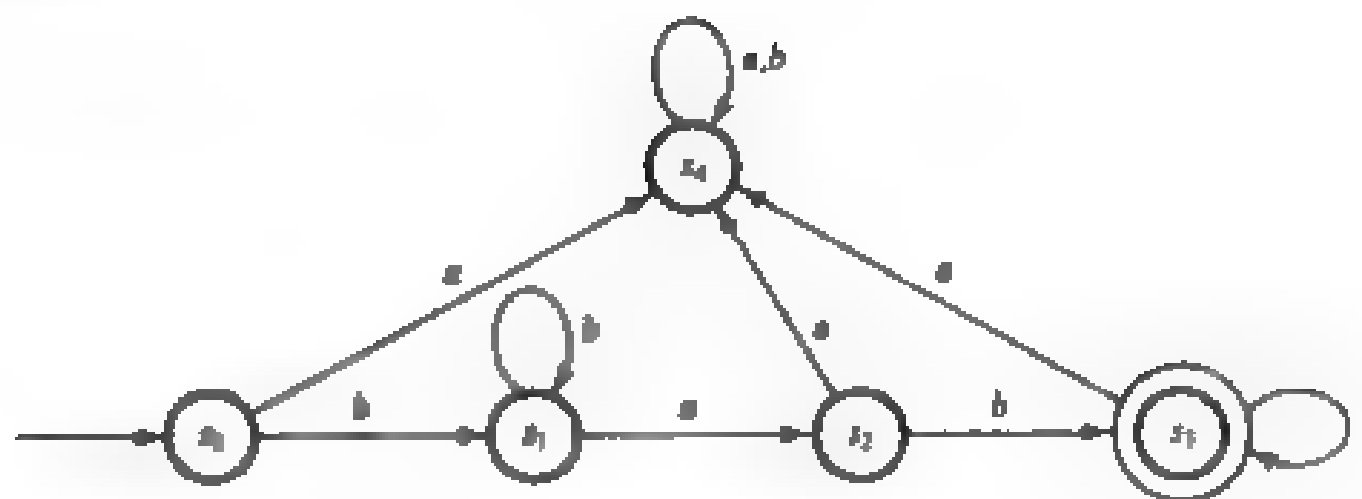



Figura 12-14

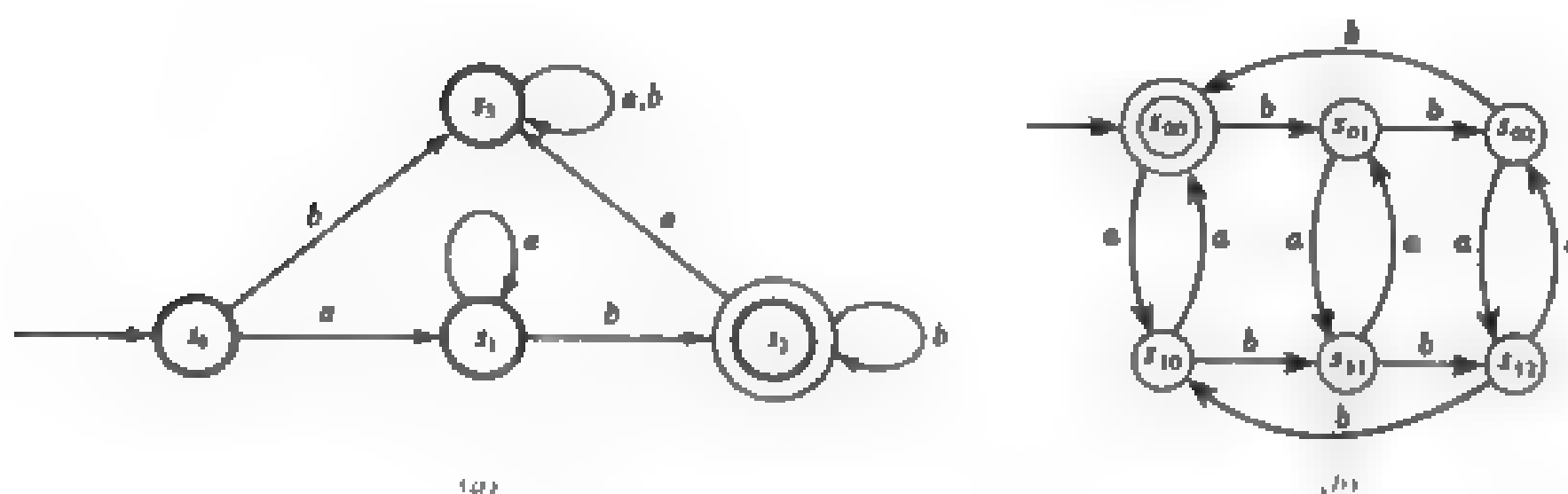



Figura 12-15

12.47 (a) Tipo 2; (b) Tipo 0; (c) Tipo 3.

12.48 $S \to (a, b, aB, bA), A \to (bA, ab, a, b), B \to (b, bA)$.

12.49 $S \to (AAB, ABA, BAA), A \to (a, BAAA, ABAA, AABA, AAAB), B \to (b, BBAA, BABA, aBAAB, ABAB, AABB)$

12.50 $S \to (aA, bB), A \to (aB, bA, a), B \to (bB, aA, b)$.

12.51 $S \to (aSa, b)$.

12.53 $L = \{ab^{2n}c \mid n \geq 0\}$.

12.54 $L = \{a^ncb^n \mid n > 0\}$

12.55 (a) $\langle S\rangle ::= a\langle A\rangle\langle B\rangle \mid \langle A\rangle\langle B\rangle, \langle A\rangle ::= a, \langle B\rangle ::= b$.

(b) Não é definido para linguagem do Tipo 0.

(c) $\langle S\rangle ::= a\langle B\rangle, \langle B\rangle ::= b\langle B\rangle \mid b\langle A\rangle, \langle A\rangle ::= a \mid b$.

12.56 (a) $\langle S\rangle ::= a \mid a\langle A\rangle\langle S\rangle, \langle A\rangle ::= b\langle S\rangle$; (b) Ver Fig. 12-16.

Figura 12-16

12.57 (a) $w = aababa$; (b) $S \to aAB, A \to aB, B \to ba$

Máquinas de Estado Finito e Máquinas de Turing

13.1 INTRODUÇÃO

Este capítulo discute dois tipos de "máquinas". O primeiro é uma máquina de estado finito (FSM, *finite state machine*) que é semelhante a um autômato de estado finito (FSA, *finite state automaton*), exceto que a máquina de estado finito "imprime" uma saída usando um alfabeto que pode ser distinto daquele empregado na entrada. O segundo tipo é a célebre máquina de Turing, a qual pode ser empregada para definir funções computáveis.

13.2 MÁQUINAS DE ESTADO FINITO

Uma máquina de estado finito (ou máquina sequencial completa) M consiste em seis componentes.

(1) Um conjunto finito A de símbolos de entrada.
(2) Um conjunto finito S de estados "internos".
(3) Um conjunto finito Z de símbolos de saída.
(4) Um estado inicial s_0 de S
(5) Uma função de próximo-estado f de $S \times A$ em S
(6) Uma função de saída g de $S \times A$ em Z.

Tal máquina M é denotada por $M = M(A, S, Z, s_0, f, g)$, quando queremos indicar suas seis componentes.

Exemplo 13.1 O que se segue define uma máquina de estado finito M com dois símbolos de entrada, três estados internos e três símbolos de saída:

(1) $A = \{a, b\}$; (2) $S = \{s_0, s_1, s_2\}$; (3) $Z = \{x, y, z\}$; (4) Estado inicial s_0;

(5) Função de próximo-estado $f : S \times A \to S$ definida por

$$f(s_0, a) = s_1, \quad f(s_1, a) = s_2, \quad f(s_2, a) = s_0$$
$$f(s_0, b) = s_2, \quad f(s_1, b) = s_1, \quad f(s_2, b) = s_1$$

(6) Função de saída $g : S \times A \to Z$ definida por:

$$g(s_0, a) = x, \quad g(s_1, a) = x, \quad g(s_2, a) = z$$
$$g(s_0, b) = y, \quad g(s_1, b) = z, \quad g(s_2, b) = y$$

Tabela de estados e diagrama de estados de uma máquina de estado finito

Existem duas maneiras de representar uma máquina de estado finito M de forma compacta. Uma delas é por meio de uma tabela chamada de *tabela de estados* da máquina M, a outra maneira é por um grafo orientado rotulado, conhecido como o *diagrama de estados* da máquina M

A tabela de estados combina a função de próximo-estado f e a função de saída g em uma única tabela que representa a função $F : S \times A \to S \times Z$ definida como se segue:

$$F(s_i, a_j) = [f(s_i, a_j), g(s_i, a_j)]$$

Por exemplo, a tabela de estados da máquina M do Exemplo 13.1 é ilustrada na Fig. 13-1(a). Os estados são listados à esquerda da tabela com o estado inicial em primeiro lugar, e os símbolos de entrada são listados no topo da tabela. A entrada na tabela é um par (s_k, z_r), onde $s_k = f(s_i, a_j)$ é o próximo estado e $z_r = g(s_i, a_j)$ é o símbolo de saída. Assume-se que não existem símbolos de saída além daqueles que aparecem na tabela.

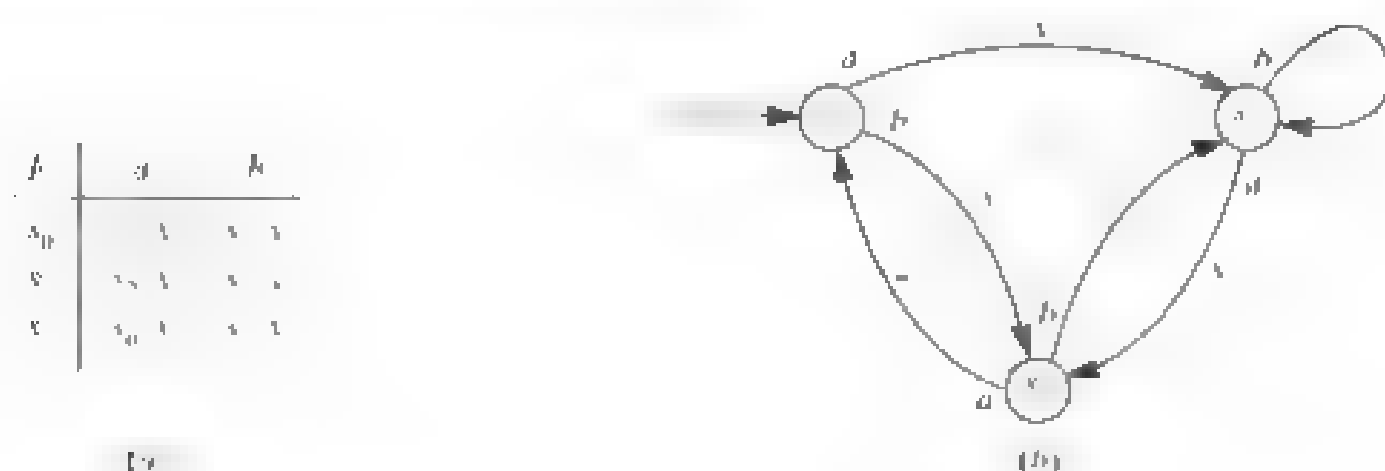



Figura 13-1

O diagrama de estados $D = D(M)$ de uma máquina de estado finito $M = M(A, S, Z, s_0, f, g)$ é um grafo orientado rotulado. Os vértices de D são os estados de M. Além disso, se

$$F(s_i, a_j) = (s_k, z_r) \quad \text{ou, equivalentemente,} \quad f(s_i, a_j) = s_k \quad \text{e} \quad g(s_i, a_j) = z_r$$

então existe um arco (flecha) de s_i a s_k, que é rotulado com o par a_j, z_r. Geralmente colocamos o símbolo a_j próximo da base da flecha (perto de s_i) e o símbolo de saída z_r próximo do centro da flecha. Também rotulamos o estado inicial s_0, desenhando uma flecha extra em s_0. Por exemplo, o diagrama de estados da máquina M no Exemplo 13.1 aparece na Fig. 13-1(b).

Fitas de entrada e saída

A discussão acima de uma máquina de estado finito M não mostra a qualidade dinâmica de M. Suponha que M recebe um string (palavra) de símbolos de entrada, digamos,

$$u = a_1 a_2 \ldots a_m$$

Visualizamos esses símbolos em uma "fita de entrada". A máquina M "lê" esses símbolos de entrada, um por um, e, simultaneamente, muda por meio de uma sequência de estados

$$v = s_0 s_1 s_2 \ldots s_m$$

onde s_0 é o estado inicial, enquanto imprime um string (palavra) de símbolos de saída

$$w = z_1 z_2 \ldots z_m$$

em uma "fita de saída". Formalmente, o estado inicial s_0 e o string de entrada u determinam os strings v e w como se segue, onde $i = 1, 2, \ldots, m$:

$$s_i = f(s_{i-1}, a_i) \quad \text{e} \quad z_i = g(s_{i-1}, a_i)$$

Exemplo 13.2 Considere a máquina M da Fig. 13-1, isto é, do Exemplo 13.1. Suponha que a entrada é a palavra

$$u = abaab$$

Calculamos a sequência v de estados e a palavra de saída w do diagrama de estados como se segue começando com o estado inicial S_0, seguimos as flechas que são rotuladas pelos símbolos de entrada, como se segue.

$$s_0 \xrightarrow{a,x} s_1 \xrightarrow{b,z} s_1 \xrightarrow{a,x} s_2 \xrightarrow{a,z} s_0 \xrightarrow{b,y} s_2$$

Isso nos leva à seguinte sequência v de estados e à palavra de saída w:

$$v = s_0 s_1 s_1 s_2 s_0 s_2 \quad \text{e} \quad w = xzxzy$$

Adição binária

Esta subseção descreve uma máquina de estado finito M que pode realizar adição binária. Adicionando 0's no início de nossos números, podemos assumir que eles têm a mesma quantia de dígitos. Se a máquina recebe a entrada

$$\begin{array}{r} 1101011 \\ +0111011 \end{array}$$

então queremos que a saída seja a soma binária 10100110. Especificamente, a entrada é o string de pares de dígitos a serem somados:

$$11, \quad 11, \quad 00, \quad 11, \quad 01, \quad 11, \quad 10, \quad b$$

onde b denota espaços em branco, e a saída deveria ser o string

$$0, \quad 1, \quad 1, \quad 0, \quad 0, \quad 1, \quad 0, \quad 1$$

Queremos também que a máquina entre com um estado chamado de "pare" quando ela termina a adição.

Os símbolos de entrada e saída são, respectivamente, como se segue:

$$A = \{00, 01, 10, 11, b\} \quad \text{e} \quad Z = \{0, 1, b\}$$

A máquina M que "construímos" tem três estados:

$$S = \{\text{continua } (c), \text{ não continua } (n), \text{ pare } (s)\}$$

Aqui n é o estado inicial. A máquina é mostrada na Fig. 13-2.

Para mostrar as limitações de nossas máquinas, estabelecemos o teorema a seguir.

Teorema 13.1: Não existe máquina de estado finito M que possa fazer multiplicação binária.

Se limitamos o tamanho dos números que multiplicamos, então tais máquinas existem. Computadores são exemplos importantes de máquinas de estado finito que multiplicam números, mas esses números são limitados quanto aos seus tamanhos.

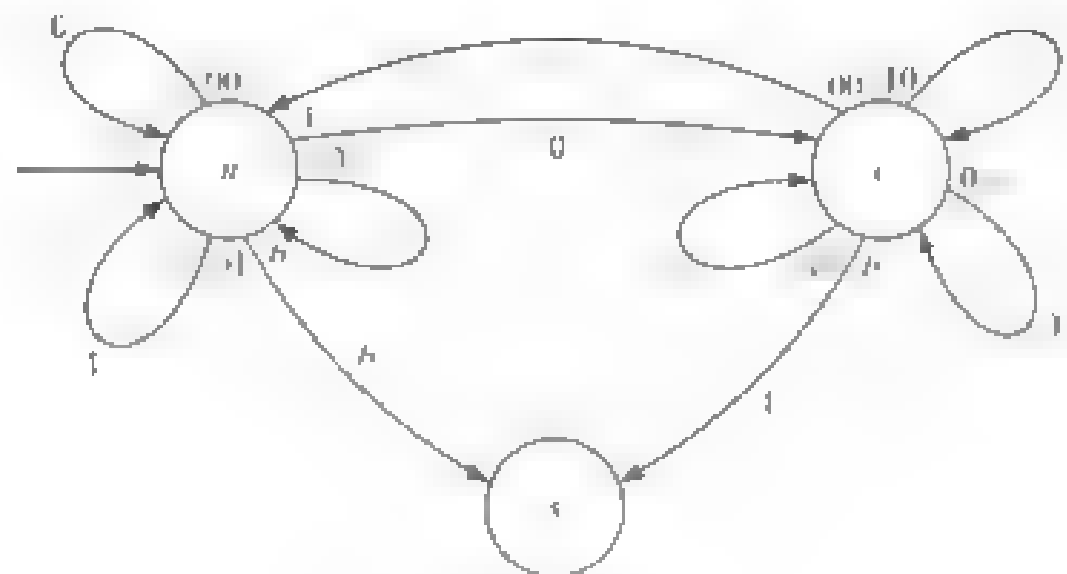



Figura 13-2

13.3 NÚMEROS DE GÖDEL

Lembre (Seção 11.5) que um inteiro positivo $p > 1$ é chamado de primo se seus únicos divisores positivos forem 1 e p. Sejam $p_1, p_2, p_3, \ldots$ os sucessivos números primos. Logo,

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11, \ldots$$

(Pelo Teorema 11.12, existe uma quantia infinita de primos.) O Teorema Fundamental da Aritmética (Teorema 11.20) estabelece que qualquer inteiro positivo $n > 1$ pode ser univocamente escrito (exceto quanto à ordem) como um produto de números primos. O lógico alemão Kurt Gödel† utilizou este resultado para codificar sequências finitas de números, bem como palavras sobre um alfabeto finito ou contável. Cada sequência ou palavra é correspondida a um inteiro positivo chamado de *número de Gödel*, da seguinte maneira.

O número de Gödel da sequência $s = (n_1, n_2, \ldots, n_k)$ de inteiros não negativos é o inteiro positivo $c(s)$, onde n_i é o expoente de p_i na decomposição em primos de $c(s)$, ou seja,

$$c(s) = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

Por exemplo,

$$s = (3, 1, 2, 0, 2) \quad \text{é codificado por} \quad c(s) = 2^3 \cdot 3 \cdot 5^2 \cdot 7^0 \cdot 11^2 = 72\,600$$

O número de Gödel de uma palavra w em um alfabeto $\{a_0, a_1, a_2, a_3, \ldots\}$ é o inteiro positivo $c(w)$, onde o subscrito da i-ésima letra de w é o expoente de p_i na decomposição em primos de $c(w)$. Por exemplo,

$$w = a_4a_1a_3a_2a_2 \quad \text{é codificada por} \quad c(w) = 2^4 \cdot 3 \cdot 5^3 \cdot 7^2 \cdot 11^2$$

(Observe que ambas as codificações são essencialmente a mesma, uma vez que podem ver uma palavra w como a sequência dos subscritos de suas letras.)

A codificação acima é essencialmente a demonstração do principal resultado desta seção.

Teorema 13.2: Suponha que um alfabeto A é contável. Então, qualquer linguagem L sobre A é também contável.
Demonstração: A codificação de Gödel é um mapa um para um $c: L \to \mathbf{N}$. Logo, L é contável.

13.4 MÁQUINAS DE TURING

Existem várias maneiras equivalentes de definir formalmente uma função "computável". Fazemos isso por meio de uma máquina de Turing M. Esta seção define formalmente uma máquina de Turing M, e a próxima seção define uma função computável.

Nossa definição de máquina de Turing emprega uma fita infinita de dois sentidos, quíntuplas e três estados de parada. Outras definições usam uma fita infinita de um sentido e/ou quádruplas, e um estado de parada. No entanto, todas as definições são equivalentes.

Definições básicas

Uma *máquina de Turing M* envolve três conjuntos disjuntos e não vazios.

(1) Um conjunto finito *fita*, onde $B = a_0$ é o símbolo "em branco":

$$A = \{a_1, a_2, \ldots, a_m\} \cup \{B\}$$

(2) Um conjunto finito *estado*, onde s_0 é o *estado inicial*:

$$S = \{s_1, s_2, \ldots, s_n\} \cup \{s_0\} \cup \{s_H, s_Y, s_N\}$$

† N. de T.: Ao contrário do que os autores afirmam, Gödel era austríaco.

Aqui s_H (PARADA) é o estado de parada, s_Y (SIM) é o estado de aceitação, e s_N (NÃO) é o estado de não aceitação.

(3) Um conjunto *direção*, onde E denota "esquerda" e D denota "direita":

$$d = \{E, D\}$$

Definição 13.1: Uma *expressão* é uma sequência finita (possivelmente vazia) de elementos de $A \cup S \cup d$.

Em outras palavras, uma expressão é uma palavra cujas letras (símbolos) derivam dos conjuntos A, S e d.

Definição 13.2: Uma *expressão de fita* é uma expressão que usa apenas elementos do conjunto fita A.

A máquina de Turing M pode ser percebida como uma cabeça de leitura/impressão que move para trás e para frente ao longo de uma fita infinita. Esta é dividida ao longo do comprimento em quadrados (células), e cada quadrado pode estar em branco ou conter um símbolo da fita. A cada passo, a máquina de Turing M está em um certo estado interno s_i lendo um dos símbolos a_j sobre a fita. Assumimos que somente um número finito de símbolos não em branco aparecem sobre a fita.

A Fig. 13-3(a) é uma representação de uma máquina de Turing M no estado s_2 lendo o segundo símbolo, sendo que $a_1a_3Ba_1a_1$ está impresso sobre a fita. (Observe novamente que B é o símbolo "em branco".) Essa representação pode ser denotada pela expressão $\alpha = a_1s_2a_3Ba_1a_1$, onde escrevemos o estado s_2 de M antes do símbolo a_3 que M está lendo. Observe que α é uma expressão que emprega apenas o alfabeto da fita A, exceto para o símbolo de estado s_2 que não está no final da expressão, uma vez que ele aparece antes do símbolo de fita a_3 que M está lendo. A Fig. 13-3 mostra duas outras ilustrações informais e suas correspondentes expressões.

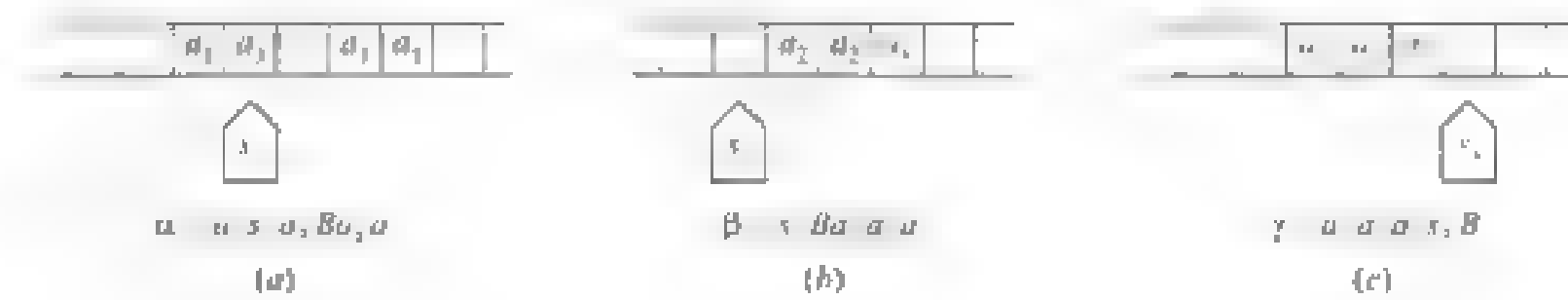



Figura 13-3

A seguir as definições formais.

Definição 13.3: Uma *imagem* α é uma expressão como a que se segue, onde P e Q são expressões de fita (possivelmente vazias):

$$\alpha = Ps_ia_kQ$$

Definição 13.4: Seja $\alpha = Ps_ia_kQ$ uma imagem. Dizemos que a máquina de Turing M *está no estado s_i lendo a letra a_k* e que *a expressão sobre a fita* é Pa_kQ, ou seja, sem seu símbolo de estado s_i.

Como mencionado acima, em cada passo ao longo do tempo a máquina de Turing M está em um certo estado s_i e está lendo um símbolo de fita a_k. A máquina de Turing M é capaz de realizar as três tarefas a seguir simultaneamente:

(i) M apaga o símbolo lido a_k e escreve em seu lugar um símbolo de fita a_l (onde permitimos que $a_l = a_k$).

(ii) M muda seu estado interno s_i para um estado s_j (onde permitimos que $s_j = s_i$.)

(iii) M move um quadrado para a esquerda ou um quadrado para a direita.

A ação recém-executada por M pode ser descrita por uma expressão de cinco letras chamada de quíntupla, a qual definimos abaixo.

Definição 13.5: Uma quíntupla q é uma expressão de cinco letras da seguinte forma:

$$q = \left(s_i,\ a_k,\ a_l,\ s_j,\ \begin{Bmatrix} L \\ R \end{Bmatrix}\right)$$

Ou seja, a primeira letra de q é um símbolo de estado, a segunda é um símbolo de fita assim como a terceira, a quarta é um símbolo de estado e a última é um símbolo de direção L (esquerda) ou R (direita).

A seguir, apresentamos a definição formal de uma máquina de Turing.

Definição 13.6: Uma máquina de Turing M é um conjunto finito de quíntuplas, tal que:

(i) Nenhuma duas quíntuplas começa com as mesmas duas letras.

(ii) Nenhuma quíntupla começa com s_H, s_Y ou s_N.

A condição (i) na definição garante que a máquina M não pode fazer mais do que uma coisa em qualquer passo, e a condição (ii) garante que M para nos estados s_H, s_Y ou s_N.

A seguir apresentamos uma definição alternativa equivalente.

Definição 13.6: A máquina de Turing M é uma função parcial de

$$S\backslash\{s_H, s_Y \text{ ou } s_N\} \times A \quad \text{em} \quad A \times S \times d$$

O termo função parcial significa apenas que o domínio de M é um subconjunto de $S\backslash\{s_H, s_Y \text{ ou } s_N\} \times A$.

A ação da máquina de Turing descrita acima pode agora ser definida formalmente.

Definição 13.7: Sejam α e β imagens. Escrevemos

$$\alpha \rightarrow \beta$$

se um dos itens a seguir for válido, onde a, b e c são letras de fita e P e Q são expressões de fita (possivelmente vazias):

(i) $\alpha = Ps_i acQ$, $\beta = Pbs_j cQ$ e M contém a quíntupla $q = s_i abs_j R$.

(ii) $\alpha = Pcs_i aQ$, $\beta = Ps_j cbQ$ e M contém a quíntupla $q = s_i abs_j L$.

(iii) $\alpha = Ps_i a$, $\beta = Pbs_j B$ e M contém a quíntupla $q = s_i abs_j R$

(iv) $\alpha = s_i aQ$, $\beta = s_j BbQ$ e M contém a quíntupla $q = s_i abs_j L$.

Observe que, em todos os quatro casos, M substitui a na fita por b (onde permitimos que $b = a$), e M muda seu estado de s_i para s_j (onde permitimos que $s_j = s_i$). Além disso:

(i) Aqui M se move à direita.

(ii) Aqui M se move à esquerda.

(iii) Aqui M se move à direita, contudo, uma vez que M está escaneando a letra na extrema direita, é necessário adicionar o símbolo em branco B à direita.

(iv) Aqui M se move à esquerda, contudo, uma vez que M está escaneando a letra na extrema esquerda, é necessário adicionar o símbolo em branco B à esquerda.

Definição 13.8: Uma imagem α é dita *terminal* se não existe uma imagem β tal que $\alpha \rightarrow \beta$.

Em particular, qualquer imagem α em um dos três estados de parada deve ser terminal, uma vez que nenhuma quíntupla começa com s_H, s_Y ou s_n.

Computando com uma máquina de Turing

Acima está uma descrição estática (de um só passo) de uma máquina de Turing M. Agora discutimos sua dinâmica.

Definição 13.9: Uma *computação* de uma máquina de Turing é uma sequência de imagens $\alpha_1, \alpha_2, \ldots, \alpha_m$ tal que $\alpha_{i-1} \rightarrow \alpha_i$, para $i = 1, 2, \ldots, m$, e α_m é uma imagem terminal.

Em outras palavras, uma computação é uma sequência

$$\alpha_0 \rightarrow \alpha_1 \rightarrow \alpha_2 \rightarrow \ldots \rightarrow \alpha_m$$

que não pode ser estendida, uma vez que α_m é terminal. Assumimos que (α) denota a imagem final de uma computação que começa com α. Logo, $(\alpha_0) = \alpha_m$ na computação acima.

Máquinas de Turing com entrada

A definição a seguir se aplica.

Definição 13.10: Uma *entrada* para uma máquina de Turing M é uma expressão de fita W. A *imagem inicial* para uma entrada W é $\alpha(W)$, onde $\alpha(W) = s_0(W)$.

Observe que a imagem inicial $\alpha(W)$ da entrada W é obtida pela colocação do estado inicial s_0 na frente da expressão W da fita de entrada. Em outras palavras, a máquina de Turing M começa com seu estado inicial s_0 e está escaneando a primeira letra de W.

Definição 13.11: Sejam M uma máquina de Turing e W uma entrada. Dizemos que M para em W se existe uma computação começando com a imagem inicial $\alpha(W)$.

Isto é, dada uma entrada W, podemos formar a imagem inicial $\alpha(W) = s_0(W)$ e aplicar M para obter a sequência

$$\alpha(W) \to \alpha_1 \to \alpha_2 \to \ldots$$

Duas coisas podem acontecer:

(1) ***M* para em *W*.** Isto é, a sequência termina com alguma imagem terminal α_r.

(2) ***M* não para em *W*.** Isto é, a sequência nunca termina.

Gramáticas e máquinas de Turing

Máquinas de Turing podem ser usadas para reconhecer linguagens. Especificamente, suponha que M é uma máquina de Turing com conjunto de fita A. Seja L o conjunto de palavras W em A tal que M para no estado de aceitação s_Y quando W está na entrada. Escrevemos, então, $L = L(M)$ e dizemos que M reconhece a linguagem L. Logo, uma entrada W não pertence a $L(M)$ se M não para em W ou se M para em W, mas não no estado de aceitação s_Y.

O Teorema a seguir é o principal resultado desta subseção, mas sua demonstração vai além do objetivo deste texto.

Teorema 13.3: Uma linguagem L é reconhecível por uma máquina de Turing M se, e somente se, L é uma linguagem tipo 0.

Observação: A razão para os três estados de parada é que s_Y e s_N são usados para reconhecimento de linguagens, enquanto s_H é usado para computações discutidas na próxima seção.

Exemplo 13.3 Suponha que uma máquina de Turing M com conjunto de fita $A = \{a, b, c\}$ contém as quatro quíntuplas a seguir:

$$q_1 = s_0aas_0R, \quad q_2 = s_0bbs_0R, \quad q_3 = s_0BBs_NR, \quad q_4 = s_0ccs_YR$$

(a) Suponha que $W = W(a, b, c)$ é uma entrada sem c's.

Segundo as quíntuplas q_1 e q_2, M fica no estado s_0 e move-se para a direita até encontrar um símbolo em branco B. Em seguida, M muda seu estado para o de não aceitação s_N e para.

(b) Suponha que $W = W(a, b, c)$ é uma entrada com pelo menos um símbolo c.

Segundo a quíntupla q_4, quando M encontra inicialmente o primeiro c em W, ela muda seu estado para o de aceitação s_Y e para.

Logo, M reconhece a linguagem L de todas as palavras W em a, b e c com, pelo menos, uma letra c. Isto é, $L = L(M)$

13.5 FUNÇÕES COMPUTÁVEIS

Funções computáveis são definidas no conjunto de inteiros não negativos. Alguns textos usam N para denotar o referido conjunto. Nós usamos N para denotar o conjunto de inteiros positivos e empregamos a notação

$$\mathbf{N}_0 = \{0, 1, 2, 3, \ldots\}$$

Ao longo desta seção, os termos número, inteiro e inteiro não negativo são usados como sinônimos. A seção precedente descreveu a maneira como uma máquina de Turing M manipula e reconhece os dados de caracteres. Aqui, mostramos como M manipula dados numéricos. Em primeiro lugar, contudo, precisamos ser capazes de representar nossos números com o conjunto de fita A. Escreveremos 1 para o símbolo fita a_1 e 1^n para $111 \ldots 1$, onde 1 ocorre n vezes.

Definição 13.12: Cada número n será representado pela expressão de fita $\langle n \rangle$, onde $\langle n \rangle = 1^{n+1}$. Logo:

$$\langle 4 \rangle = 11111 = 1^5, \quad \langle 0 \rangle = 1, \quad \langle 2 \rangle = 111 = 1^3.$$

Definição 13.13: Seja E uma expressão. Então $[E]$ denotará o número de vezes que 1 ocorre em E. Logo,

$$[11Bs_2a_3111Ba_4] = 5, \quad [a_4s_2Ba_2] = 0, \quad [\langle n \rangle] = n + 1.$$

Definição 13.14: Uma função $f: \mathbf{N}_0 \to \mathbf{N}_0$ é computável se existir uma máquina de Turing M tal que, para todo inteiro n, M para em $\langle n \rangle$ e

$$f(n) = [\text{term}(\alpha(\langle n \rangle))]$$

Dizemos, então, que M computa f.

Isto é, dada uma função f e um inteiro n, colocamos a entrada $\langle n \rangle$ e aplicamos M. Se M sempre para em $\langle n \rangle$ e o número de 1's na imagem final é igual a $f(n)$, então f é uma função computável e dizemos que M computa f.

Exemplo 13.14 A função $f(n) = n + 3$ é computável. A entrada é $W = 1^{n+1}$. Logo, precisamos apenas adicionar dois 1's à entrada. Uma máquina de Turing M que calcula f é descrita a seguir:

$$M = \{q_1, q_2, q_3\} = \{s_0 1 s_0 L, \quad s_0 B 1 s_1 L, \quad s_1 B 1 s_H L\}$$

Observe que:

(1) q_1 move a máquina M à esquerda.

(2) q_2 escreve 1 no quadrado em branco B e move M à esquerda.

(3) q_3 escreve 1 no quadrado em branco B e para M.

Consequentemente, para qualquer inteiro positivo n,

$$s_0 1^{n+1} \to s_0 B 1^{n+1} \to s_1 B 1^{n+2} \to s_H B 1^{n+3}$$

Logo, M computa $f(n) = n + 3$. É claro que, para qualquer inteiro positivo k, a função $f(n) = n + k$ é computável.

O teorema a seguir é válido.

Teorema 13.4: Suponha que $f: \mathbf{N}_0 \to \mathbf{N}_0$ e $g: \mathbf{N}_0 \to \mathbf{N}_0$ são computáveis. Então a função composição $h = g \circ f$ é computável.

Indicamos a demonstração desse teorema aqui. Suponha que M_f e M_g são máquinas de Turing que computam f e g, respectivamente. Dada a entrada $\langle n \rangle$, aplicamos M_f a $\langle n \rangle$ para finalmente obter uma expressão E com $[E] = f(n)$. Arranjamos, então, que $E = s_0 1^{f(n)}$. Precisamos agora adicionar 1 a E para obter $E' = s_0 1 1^{f(n)}$, e aplicamos M_g a E'. Isso implica E'' onde $[E''] = g(f(n)) = (g \circ f)(n)$, como pedido.

Funções de várias variáveis

Esta subseção define uma função computável $f(n_1, n_2, \ldots, n_k)$ de k variáveis. Em primeiro lugar, precisamos representar a lista $m = (n_1, n_2, \ldots, n_k)$ em nosso alfabeto A.

Definição 13.15: Cada lista $m = (n_1, n_2, \ldots, n_k)$ de k inteiros é representada pela expressão

$$\langle m \rangle = \langle n_1 \rangle B \langle n_2 \rangle B \cdots B \langle n_k \rangle$$

Por exemplo, $\langle (2, 0, 4) \rangle = 111B1B11111 = 1^3B1^1B1^5$.

Definição 13.16: Uma função $f(n_1, n_2, \ldots, n_k)$ de k variáveis é computável se existir uma máquina de Turing M tal que, para toda lista $m = (n_1, n_2, \ldots, n_k)$, M para em $\langle m \rangle$ e

$$f(m) = [\text{term}(\alpha(\langle m \rangle))]$$

Dizemos, então, que M computa f.

A definição é análoga à Definição 13.14 para uma variável.

Exemplo 13.15 A função adição $f(m, n) = m + n$ é computável. A entrada é $W = 1^{m+1}B1^{n+1}$. Logo, precisamos apenas apagar dois dos 1's. Uma máquina de Turing M que computa f é descrita a seguir:

$$M = \{q_1, q_2, q_3, q_4\} = \{s_0 1Bs_1 R, \quad s_1 1Bs_H R, \quad s_1 BBs_2 R, \quad s_2 1Bs_H R\}$$

Observe que

(1) q_1 apaga o primeiro 1 e move M à direita.

(2) Se $m \neq 0$, então q_2 apaga o segundo 1 e para M.

(3) Se $m = 0$, q_3 move M à direita, passando o espaço em branco B.

(4) q_4 apaga o 1 e para M

Consequentemente, se $m \neq 0$, temos:

$$s_0 1^{m+1}B1^{n+1} \to s_1 1^m B1^{n+1} \to s_H 1^{m-1}B1^{n+1}$$

mas, se $m = 0$ e $m + n = n$, temos

$$s_0 1B1^{n+1} \to s_1 B1^{n+1} \to s_2 1^{n+1} \to s_H 1^n$$

Logo, M computa $f(m, n) = m + n$.

Problemas Resolvidos

Máquinas de estado finito

13.1 Seja M uma máquina de estado finito, com a tabela de estados aparecendo na Fig. 13-4(a).

(a) Encontre o conjunto de entrada A, o conjunto de estado S, o conjunto de saída Z e o estado inicial.

(b) Esboce o diagrama de estado $D = D(M)$ de M.

(c) Suponha que $w = aababaabbab$ é uma palavra de entrada (*string*). Encontre a palavra de saída v correspondente.

(a) Os símbolos de entrada estão no topo da tabela, os estados estão listados na esquerda e os símbolos de saída aparecem na tabela. Logo:

$$A = \{a, b\}, \quad S = \{s_0, s_1, s_2, s_3\}, \quad Z = \{x, y, z\}$$

O estado s_0 é o inicial, uma vez que é o primeiro estado listado na tabela.

F	a	b
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

(a)

(b)

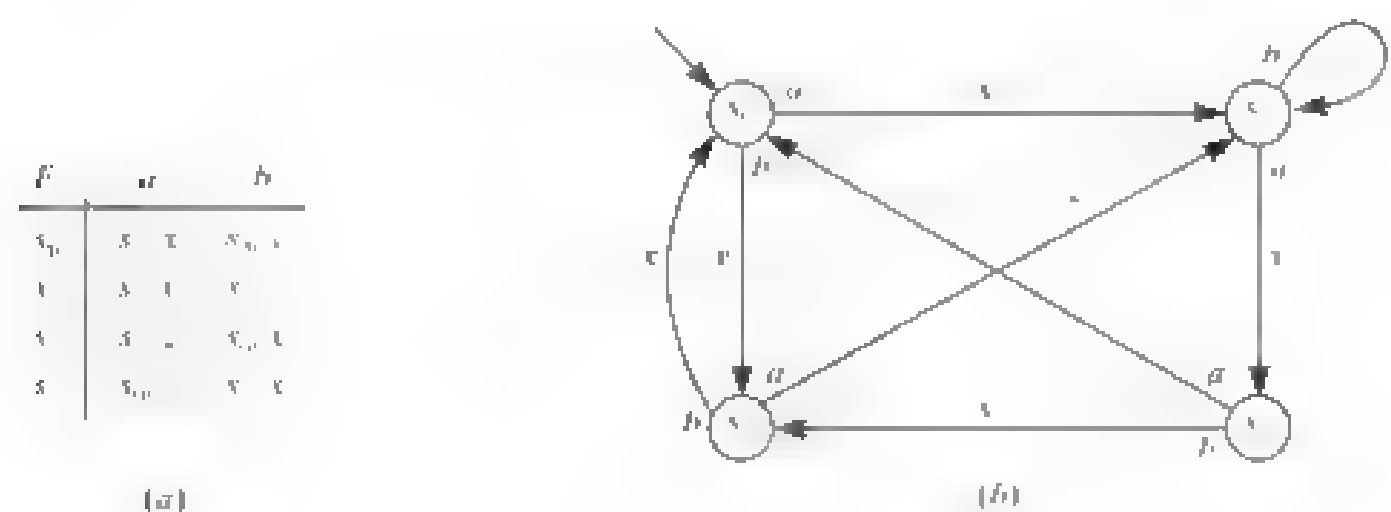



Figura 13-4

(b) O diagrama de estado $D = D(M)$ aparece na Fig. 13-4(b). Note que os vértices de D são os estados de M. Suponha que $F(s_i, a_j) = (s_k, z_r)$. (Isto é, $f(s_i, a_j) = s_k$ e $g(s_i, a_j) = z_r$.)

Então existe uma aresta orientada de s_i para s_k rotulada pelo par a_j, z_r. Usualmente, o símbolo de entrada a_j é colocado perto da base da flecha (próximo de s_i), e o símbolo de saída z_r é colocado próximo do centro da flecha.

(*d*) Começando no estado inicial s_0, movemos de estado para estado segundo as flechas que são rotuladas, respectivamente, pelos símbolos de entrada dados, como se segue:

$$s_0 \xrightarrow{a} s \xrightarrow{a} s \xrightarrow{b} s \xrightarrow{a} s \xrightarrow{b} s_1 \xrightarrow{a} s \xrightarrow{a} s \xrightarrow{b} s \xrightarrow{b} s_0 \xrightarrow{a} s \xrightarrow{b} s$$

Os símbolos de saída nas flechas acima implicam a palavra de saída pedida $v = xyxzzyzxxz$.

13.2 Seja M a máquina de estado finito com conjunto de entrada $A = \{a, b\}$, conjunto de saída $Z = \{x, y, z\}$ e o diagrama de estado $D = D(M)$ na Fig. 13-5(*a*).

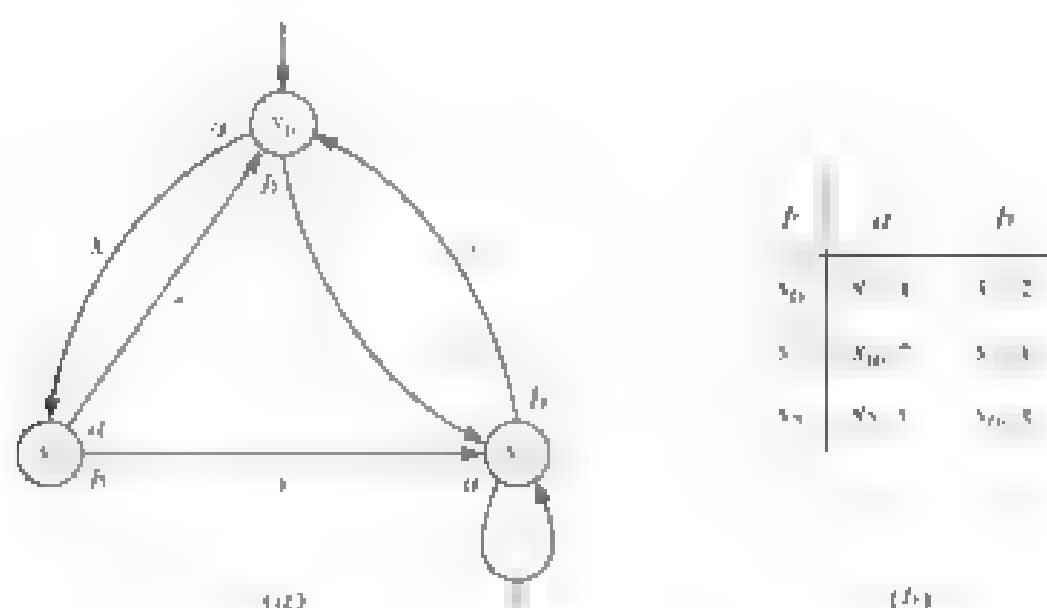



Figura 13-5

(*a*) Construa a tabela de estados de M.

(*b*) Encontre a palavra de saída v se a entrada é a palavra: (i) $w = a^2b^2abab$; (ii) $w = abab^3a^2$.

(*a*) A tabela de estados aparece na Fig. 13-5(*b*). Uma vez que s_0 é o estado inicial, ele é listado no topo. Além disso, $F(s_i, a_j) = (s_k, z_r)$ se existe uma aresta orientada de s_i a s_k rotulada pelo par a_j, z_r.

(*b*) Mova de estado para estado pelas flechas que são rotuladas, respectivamente, pelos símbolos de entrada dados para obter a saída a seguir: (i) $v = xz^2x^2y^2x$; (ii) $v = xy^2zzxx^2z$.

Máquinas de Turing

13.3 Seja M uma máquina de Turing. Determine a imagem α correspondente a cada situação.

(*a*) M está no estado s_3 e escaneando a terceira letra da expressão fita $w = aabca$.

(*b*) M está em um estado s_2 e escaneando a última letra da expressão fita $w = abca$.

(*c*) A entrada é a expressão de fita $w = 1^4B1^2$.

A imagem α é obtida pela colocação do símbolo de estado antes da letra ser escaneada. Inicialmente, M está em um estado s_0, escaneando a primeira letra de uma entrada. Logo:

(*a*) $\alpha = aas_3bca$; (*b*) $\alpha = abcs_2a$; (*c*) $\alpha = s_01111B11$

13.4 Suponha que $\alpha = aas_2ba$ é uma imagem. Encontre β tal que $\alpha \to \beta$ se a máquina de Turing M possui a quíntupla q em que: (*a*) $q = s_2bas_1L$; (*b*) $q = s_2bbs_3R$; (*c*) $q = s_2bas_2R$; (*d*) $q = s_3abs_1L$.

(*a*) Aqui M apaga b e escreve a, muda seu estado para s_1 e move-se à esquerda. Logo, $\beta = as_1aaa$.

(*b*) Aqui M não muda a letra escaneada b, muda seu estado para s_3 e move-se à direita. Logo, $\beta = aabs_3a$.

(*c*) Aqui M apaga b e escreve a, mantém seu estado s_2 e move-se à direita. Logo, $\beta = aaas_2a$.

(*d*) Aqui q não possui efeito sobre α, uma vez que q não começa com s_2b.

13.5 Sejam $A = \{a, b\}$ e $L = \{a^r b^s \mid r > 0, s > 0\}$, isto é, L consiste em todas as palavras W que começam com um ou mais a's seguidos por um ou mais b's. Encontre uma máquina de Turing M que reconheça L.

A estratégia é que queremos que M: (1) mova à direita todos os a's, (2) mova à direita todos os b's, (3) pare no estado de aceitação s_Y quando encontrar o símbolo em branco B. As quíntuplas a seguir cumprem essas funções:

$$q_1 = s_0aas_1R, \quad q_2 = s_1aas_1R, \quad q_3 = s_1bbs_2R, \quad q_4 = s_2bbs_2R, \quad q_5 = s_2BBs_YR$$

Especificamente, q_1 e q_2 cumprem com (1), q_3 e q_4 cumprem com (2) e q_5 cumpre com (3).

Contudo, também queremos que M não aceite uma palavra de entrada W que não pertença a L. Logo, também precisamos das quíntuplas a seguir:

$$q_6 = s_0BBs_NR, \; q_7 = s_0bbs_NR, \; q_8 = s_1BBs_NR, \; q_9 = s_2aas_NR$$

Aqui, q_6 é usada se a entrada $W = \lambda = B$, a palavra vazia, q_7 é usada se a entrada W é uma expressão que comece com b; q_8 é usada se a entrada W contém apenas a's, e q_9 é usada se a entrada W contém a letra a seguida de uma letra b.

Funções computáveis

13.6 Encontre $\langle m \rangle$ se: (*a*) $m = 5$; (*b*) $m = (4, 0, 3)$; (*c*) $m = (3, -2, 5)$.

Lembre que $\langle n \rangle = 1^{n+1} = 11^n$ e $\langle (n_1, n_2, \ldots, n_r) \rangle = \langle n_1 \rangle B \langle n_2 \rangle B \cdots B \langle n_r \rangle$. Logo:

(*a*) $\langle m \rangle = 1^6 = 111111$

(*b*) $\langle m \rangle = 1^5B1^1B1^4 = 11111B1B1111$

(*c*) $\langle m \rangle$ não é definida para inteiros negativos.

13.7 Encontre $[E]$ para as expressões:

(*a*) $E = a11s_2Bb111$; (*c*) $E = \langle m \rangle$, onde $m = (4, 1, 2)$;

(*b*) $E = aas_3bb$; (*d*) $E = \langle m \rangle$, onde $m = (n_1, n_2, \ldots, n_r)$.

Lembre que $[E]$ conta o número de 1's em E. Então:

(*a*) $[E] = 5$. (*b*) $[E] = 0$; (*c*) $[E] = 10$, onde $E = 1^5B1^2B1^3$;

(*d*) $[E] = n_1 + n_2 + \cdots + n_r + r$, uma vez que o número de 1's contribuído por n_k a E é $n_k + 1$.

13.8 Seja f uma função $f(n) = n - 1$ quando $n > 0$ e $f(0) = 0$. Mostre que f é computável.

Precisamos encontrar uma máquina de Turing M que compute f. Especificamente, queremos que M apague dois dos 1's na entrada $\langle n \rangle$ quando $n > 0$, mas apenas um 1 quando $n = 0$. Isso é conseguido com as quíntuplas a seguir:

$$q_1 = s_01Bs_1R, \quad q_2 = s_1BBs_HR, \quad q_3 = s_11Bs_HR$$

Aqui q_1 apaga o primeiro 1 e move M para a direita. Se existe apenas um 1, então M está agora escaneando um símbolo em branco B e q_2 diz ao computador para parar. Caso contrário, q_3 apaga o segundo 1 e para M.

13.9 Seja f a função $f(x, y) = y$. Mostre que f é computável.

Precisamos encontrar uma máquina de Turing M que compute f. Especificamente, queremos que M apague todos os 1's de $\langle x \rangle$ e um dos 1's de $\langle y \rangle$. Isso é conseguido com as quíntuplas a seguir:

$$q_1 = s_01Bs_1R, \quad q_2 = s_0BBs_1R, \quad q_3 = s_11Bs_HR$$

Aqui q_1 apaga todos os 1's em $\langle x \rangle$ enquanto move M para a direita. Quando M escaneia o espaço em branco B, q_2 muda o estado de M de s_0 para s_1 e move M para a direita. Então q_3 apaga o primeiro 1 em $\langle y \rangle$ e para M.

Problemas Complementares

Máquinas de estado finito

13.10 Seja M a máquina de estado finito com a tabela de estados que aparece na Fig. 13-6(*a*).

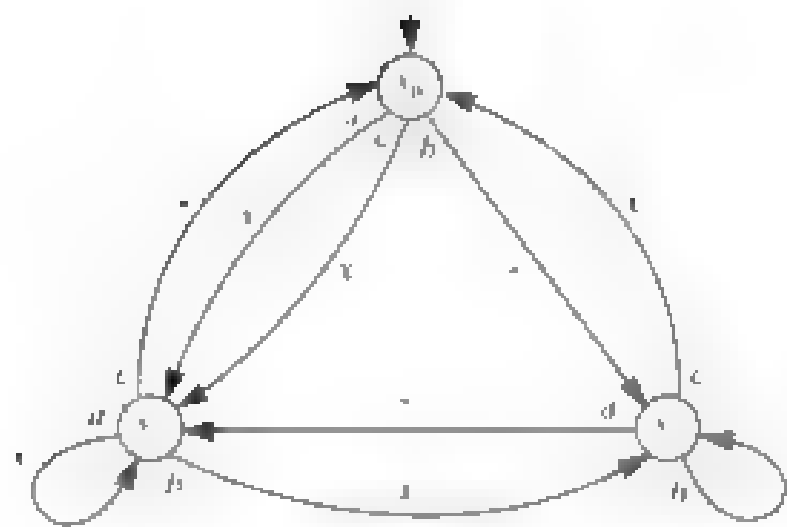



Figura 13-6

(a) Encontre o conjunto de entrada A, o conjunto de estado S, o conjunto de saída Z e o estado inicial de M.

(b) Esboce o diagrama de estados $D = D(M)$ de M

(c) Encontre a palavra de saída v se a entrada é a palavra. (i) $w = ab^3a^2ba^3b$, (ii) $w = a^2b^2ab^2a^2b$.

13.11 Seja M a máquina de estado finito com conjunto de entrada $A = \{a, b, c\}$, conjunto de saída $Z = \{x, y, z\}$ e o diagrama de estados $D = D(M)$ na Fig. 13-6(b).

(a) Construa a tabela de estados de M

(b) Encontre a palavra de saída v se a entrada é a palavra (i) $w = a^2c^2b^2cab^3$, (ii) $w = ca^2b^2ac^2ab$

13.12 Seja M uma máquina de estado finito com conjunto de entrada $A = \{a, b\}$, conjunto de saída $Z = \{x, y, z\}$ e diagrama de estados $D = D(M)$ na Fig. 13-7(a). Encontre a palavra de saída v se a entrada é a palavra.

(a) $w = ab^3a^2ba^3b$; (b) $w = aba^2b^2ab^2a^2ba^2$.

13.13 Repita o Problema 13.12 para o diagrama de estados $D = D(M)$ na Fig. 13-7(b).

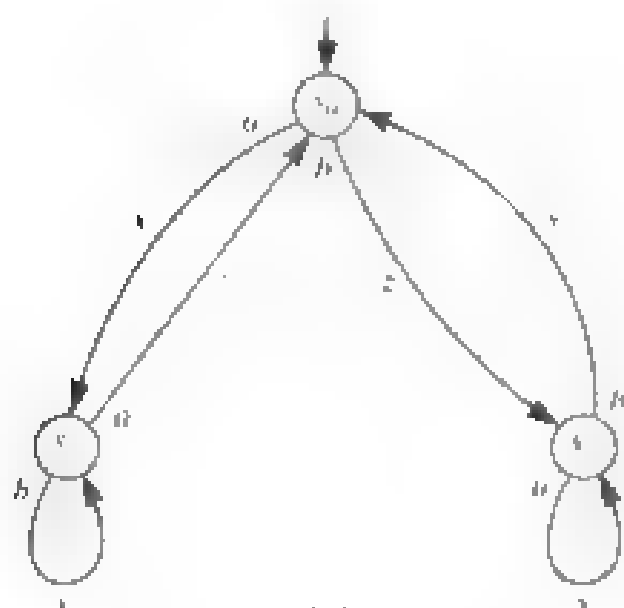
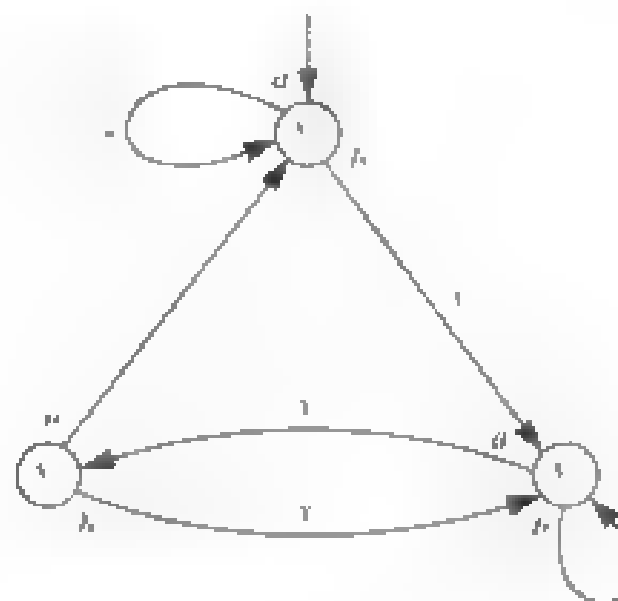



Figura 13-7

Máquinas de Turing

13.14 Seja M uma máquina de Turing. Determine a imagem α correspondente a cada uma das situações.

(a) M está no estado s_2 e escaneando a terceira letra da expressão de fita $w = abbaa$.

(b) M está no estado s_3 e escaneando a última letra da expressão de fita $w = aabb$

(c) A entrada é a palavra $W = a^3b^3$.

(d) A entrada é a expressão fita $W = (3, 2)$

13.15 Suponha que $\alpha = abs_2aa$ é uma imagem. Encontre β tal que $\alpha \to \beta$ se a máquina de Turing M possui a quíntupla q, onde

(a) $q = s_2abs_1R$; (b) $q = s_2aas_3L$; (c) $q = s_2abs_2R$;

(d) $q = s_2abs_3L$; (e) $q = s_3abs_2R$; (f) $q = s_2aas_2L$.

13.16 Repita o Problema 13.15 para a imagem $\alpha = s_2aBab$.

13.17 Encontre as imagens distintas $\alpha_1, \alpha_2, \alpha_3$ e α_4 e uma máquina de Turing M tal que a sequência a seguir não termine:

$$\alpha_1 \to \alpha_2 \to \alpha_3 \to \alpha_4 \to \alpha_1 \to \alpha_2 \to \cdots$$

13.18 Suponha que $\alpha \to \beta_1$ e $\alpha \to \beta_2$. É necessário que $\beta_1 = \beta_2$?

13.19 Suponha que $\alpha = \alpha(W)$ para alguma entrada W, e suponha que $\alpha \to \beta \to \alpha$. É possível que M reconheça W?

13.20 Seja $A = \{a, b\}$. Encontre uma máquina de Turing M que reconheça a linguagem $L = \{ab^n : n > 0\}$, isto é, onde L consista em todas as palavras W começando com um a e que seja seguido por um ou mais b's.

13.21 Seja $A = \{a, b\}$. Encontre uma máquina de Turing M que reconheça a linguagem finita $L = \{a, a^2\}$, isto é, onde L consista nas duas primeiras potências diferentes de zero de a.

Funções computáveis

13.22 Encontre $\langle m \rangle$ se: (a) $m = 6$; (b) $m = (5, 0, 3, 1)$; (c) $m = (0, 0, 0)$; (d) $m = (2, 3, -1)$.

13.23 Encontre $[E]$ para as expressões: (a) $E = 111s_2aa1B111$, (b) $E = a11bs_1Bb$, (c) $E = \langle m \rangle$, onde $m = (2, 5, 4)$.

13.24 Seja f a função $f(n) = n - 2$ quando $n > 1$ e $f(n) = 0$ quando $n = 0$ ou 1. Mostre que f é computável.

13.25 Seja f a função $f(x, y) = x$. Mostre que f é computável.

Respostas dos Problemas Complementares

13.10 (a) $A = \{a, b\}$, $S = \{s_0, s_1, s_2\}$, $Z = \{x, y, z\}$ e s_0 é o estado inicial. (b) Veja a Fig. 13-8(a).
(c) $v = y^2zyzxzxyz$

13.11 (a) Veja a Fig. 13-8. (b) (i) $v = xyz^2x^2zx^3z^2$;
(ii) $v = xy^2xz^3xyx$.

13.12 (a) $xy^3zxyzxz^2$; (b) $xyzxy^2z^2x^2z^2y^2$.

13.13 (a) zyz^2xy^2xyzy; (b) $zyxy^2zx^2zxy^2xy$.

13.14 (a) $\alpha = abs_2baa$; (b) $\alpha = aabs_3b$; (c) $\alpha = s_0aaabbb$;
(d) $\alpha = s_01111B111$.

13.15 (a) $\beta = abbs_3a$; (b) $\beta = as_3baa$; (c) $\beta = abbs_2a$;
(d) $\beta = as_3bba$; (e) α não é mudado por q;
(f) $\beta = as_2baa$.

13.16 (a) $\beta = bs_1Bab$; (b) $\beta = s_3BaBab$; (c) $\beta = bs_2Bab$;
(d) $\beta = s_3BbBab$; (e) α não é mudado por q;
(f) $\beta = s_2BaBab$.

13.17 $\alpha_1 = s_0ab$, $\alpha_2 = bs_1b$, $\alpha_3 = s_2bb$, $\alpha_4 = as_3b$;
$q_1 = s_0abs_1R$, $q_2 = s_1bbs_2L$, $q_3 = s_2bas_3R$,
$q_4 = s_3bbs_0L$.

(a)

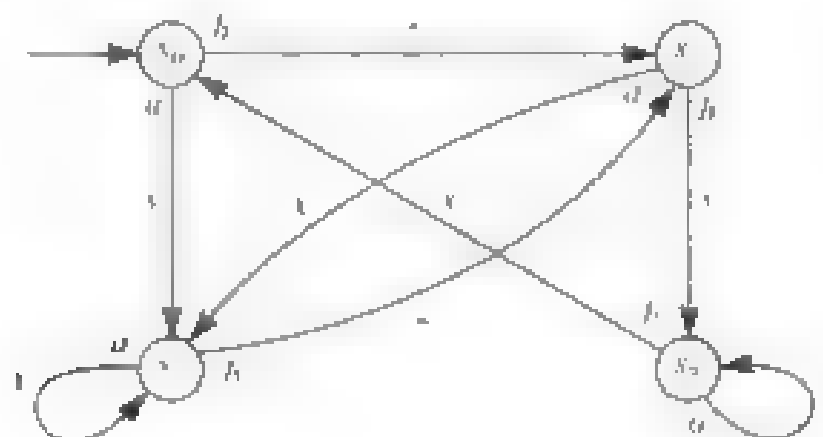
F	a	b	c
s_0	s_1, y	[illegible]	s_1, y
s_1	[illegible]	[illegible]	[illegible]
s_2	[illegible]	[illegible]	[illegible]

(b)

Figura 13-8

13.18 Sim.

13.19 Não, uma vez que $\alpha \to \beta \to \alpha \to \beta \to \alpha \to \beta \to \cdots$ nunca acaba.

13.20 $q_1 = s_0BBs_NR$ (NÃO); $q_2 = s_0bbs_NR$ (NÃO); $q_3 = s_0aas_1R$; $q_4 = s_1BBs_NR$ (NÃO); $q_5 = s_1aas_NR$ (NÃO); $q_6 = s_1bbs_NR$; $q_7 = s_2bbs_2R$; $q_8 = s_2aas_NR$ (NAO); $q_9 = s_2BBs_YR$ (SIM).

13.21 $q_1 = s_0BBs_NR$ (NÃO); $q_2 = s_0bbs_NR$ (NÃO); $q_3 = s_0aas_1R$; $q_4 = s_1BBs_YR$ (SIM); $q_5 = s_1bbs_NR$ (NÃO); $q_6 = s_1aas_2R$; $q_7 = s_2BBs_YR$ (SIM); $q_8 = s_2aas_NR$ (NÃO); $q_9 = s_2bbs_NR$ (NÃO).

13.22 (a) $(6) = 1^7$; (b) $(m) = 1^6B1B1^4B1^2$

(c) $(m) = 1B1B1$; (d) não definido.

13.23 (a) $[E] = 7$ (b) $[E] = 2$; (c) $[E] = 14$.

13.24 Estratégia: Apague os três primeiros 1's.
$q_1 = S_01Bs_1R$; $q_2 = s_1BBs_HR$ (PARE), $q_3 = S_11Bs_2R$, $q_4 = s_2BBs_HR$ (PARE); $q_5 = s_2BBs_HR$ (PARE).

13.25 Estratégia: Apague o primeiro 1 e todos os outros que vêm depois de B.
$q_1 = s_01Bs_1R$; $q_2 = S_111s_1R$; $q_3 = S_1BBs_2R$; $q_4 = S_21Bs_3R$; $q_5 = S_31Bs_3R$; $q_6 = S_3BBs_HR$ (PARE).

Conjuntos Ordenados e Reticulados

14.1 INTRODUÇÃO

Relações de ordem e de precedência aparecem em vários lugares diferentes na matemática e na ciência da computação. Este capítulo torna essas noções precisas. Definimos, também, um reticulado, que é um tipo especial de conjunto ordenado.

14.2 CONJUNTOS ORDENADOS

Suponha que R é uma relação em um conjunto S que satisfaz estas três propriedades.

[O_1] (Reflexiva) Para qualquer $a \in S$, temos aRa.

[O_2] (Antissimétrica) Se Rb e bRa, então $a = b$.

[O_3] (Transitiva) Se Rb e bRc, então aRc.

Então R é chamada de *ordem parcial* ou, simplesmente, de uma relação de *ordem*, e R tida como a relação que define uma *ordenação parcial* de S. O conjunto S com a ordem parcial é chamado de *conjunto parcialmente odenado* ou, simplesmente, um *conjunto ordenado* ou *poset* (abreviação em inglês para *partially ordered set*). Escrevemos (S, R) quando queremos especificar a relação R.

A relação de ordem mais conhecida, chamada de *ordem usual*, é a relação $\leq$ (lê-se "menor ou igual a") nos inteiros positivos **N** ou, de forma mais geral, em qualquer subconjunto dos números reais **R**. Por essa razão, uma relação de ordem parcial é usualmente denotada por $\precsim$, e

$$a \precsim b$$

é lido "*a* precede *b*". Neste caso, também escrevemos:

$a \prec b$ significa $a \precsim b$ e $a \neq b$; lê-se "*a* precede estritamente *b*".

$b \succsim a$ significa $a \precsim b$; lê-se "*b* sucede *a*".

$b \succ a$ significa $a \prec b$; lê-se "*b* sucede estritamente *a*".

$\not\precsim$, $\not\prec$, $\not\succsim$ e $\not\succ$ são autoexplicativos.

Quando não existir ambiguidade, os símbolos $\leq$, $<$, $>$ e $\geq$ são frequentemente usados no lugar de $\precsim$, $\prec$, $\succ$ e $\succsim$, respectivamente.

Exemplo 14.1

(a) Seja S qualquer coleção de conjuntos. A relação $\subseteq$ de inclusão de conjunto é uma ordem parcial sobre S. Especificamente, $A \subseteq A$ para qualquer conjunto A, se $A \subseteq B$ e $B \subseteq A$, então $A = B$, se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

(b) Considere o conjunto **N** de inteiros positivos. Dizemos "a divide b", escrito na forma $a \mid b$, se existir um inteiro c tal que $ac = b$. Por exemplo, $2 \mid 4$, $3 \mid 12$, $7 \mid 21$, e assim por diante. Essa relação de divisibilidade é uma ordem parcial de **N**.

(c) A relação "$\mid$" de divisibilidade não é uma ordenação do conjuto **Z** de inteiros. Especificaemnte, a relação não é antissimétrica. Por exemplo, $2 \mid -2$ e $-2 \mid 2$, mas $2 \neq -2$.

(d) Considere o conjunto **Z** de inteiros. Defina aRb se existe um inteiro positivo r tal que $b = a^r$. Por exemplo, $2\ R\ 8$, uma vez que $8 = 2^3$. Então R é uma ordenação parcial de **Z**.

Ordem Dual

Seja $\precsim$ qualquer ordenação parcial de um conjunto S. A relação $\succsim$, isto é, a sucede b, é também uma ordenação parcial de S; é chamada de *ordem dual*. Observe que $a \precsim b$ se, e somente se, $b \succsim a$. Logo, a odem dual $\succsim$ é o inverso da relação $\precsim$, isto é, $\succsim = \precsim^{-1}$.

Subconjuntos ordenados

Seja A um subconjunto de um conjunto ordenado S, e suponha que $a, b \in A$. Defina $a \precsim b$ como elementos de A quando $a \precsim b$ forem elementos de A. Isso define uma ordenação parcial de A chamada de *ordem induzida* em A. O subconjunto S com a ordem induzida é chamado de *subconjunto ordenado* de S. A menos que seja explícito o contrário, qualquer subconjunto de um conjunto ordenado S será tratado como um subconjunto ordenado de S.

Quase-ordem

Suponha que $\prec$ é uma relação em um conjunto S que satisfaz as duas propriedades a seguir:

[Q_1] (Irreflexiva) **Para qualquer $a \in A$, temos $a \nprec a$.**
[Q_2] (Transitiva) **Se $a \prec b$, e $b \prec c$, então $a \prec c$.**

Então $\prec$ é chamada de *quase-ordem* em S.

Existe uma relação próxima entre ordens parciais e quase-ordens. Especificamente, se $\precsim$ é uma ordem parcial em um conjunto S, e definimos $a \prec b$ para dizer $a \precsim b$, mas $a \neq b$, então $\prec$ é uma quase-ordem em S. Reciprocamente, se $\prec$ é uma quase-ordem em um conjunto S e definimos $a \precsim b$ para dizer $a \prec b$ ou $a = b$, então $\precsim$ é uma ordem parcial em S. Isso nos permite alternar entre uma ordem parcial e suas quase-ordens correspondentes, usando aquela que nos for mais conveniente.

Comparatividade, conjuntos linearmente ordenados

Suponha que a e b são elementos em um conjunto ordenado S. Dizemos que a e b são *comparáveis* se

$$a \precsim b \text{ ou } b \precsim a$$

isto é, se um deles precede o outro. Logo, a e b são *não comparáveis*, escrito na forma

$$a \parallel b$$

se nem $a \precsim b$ nem $b \precsim a$.

A palavra "parcial" é usada ao definirmos um conjunto parcialmente ordenado S, uma vez que alguns dos elementos de S não precisam ser comparáveis. Suponha que, por um lado, todo par de elementos de S é comparável. Então S é considerado como *totalmente ordenado* ou *linearmente ordenado*, e S é chamado de *corrente*. Embora um conjunto ordenado S possa não ser linearmente ordenado, ainda é possível que um subconjunto A de S seja linearmente ordenado. Claramente, todo subconjunto de um conjunto linearmente ordenado S precisa, também, ser linearmente ordenado.

Exemplo 14.2

(a) Considere o conjunto **N** de inteiros positivos ordenado por divisibilidade. Nesse caso, 21 e 7 são comparáveis, uma vez que $7 \mid 21$. Por outro lado, 3 e 5 não são comparáveis, uma vez que não é possível $3 \mid 5$ ou $5 \mid 3$. Logo, **N** não é linearmente ordenado por divisibilidade. Observe que $A = \{2, 6, 12, 36\}$ é um subconjunto linearmente ordenado de **N**, uma vez que $2 \mid 6$, $6 \mid 12$ e $12 \mid 36$.

(b) O conjunto **N** de inteiros positivos com a ordem usual $\leq$ (menor do que ou igual) é linearmente ordenado; logo, todo subconjunto ordenado de **N** é, também, linearmente ordenado.

(c) O conjunto potência $P(A)$ de um conjunto A com dois ou mais elementos não é linearmente ordenado por inclusão de conjuntos. Por exemplo, suponha que a e b pertencem a A. Então $\{a\}$ e $\{b\}$ são não comparáveis. Observe que o conjunto vazio $\emptyset$, $\{a\}$ e A formam um subconjunto linearmente ordenado de $P(A)$, uma vez que $\emptyset \subset \{a\} \subset A$. De forma similar, $\emptyset$, $\{b\}$ e A formam um subconjunto linearmente ordenado de $P(A)$.

Conjuntos produtos e ordem

Existem várias maneiras de definirmos uma relação de ordem no produto cartesiano de determinados conjuntos ordenados. A seguir apresentamos duas dessas maneiras.

(*a*) ***Ordem de produto***: Suponha que S e T são conjuntos ordenados. Então, a seguir, temos uma relação de ordem no conjunto produto $S \times T$, chamada de ***ordem de produto***:

$$(a, b) \precsim (a', b') \quad \text{se} \quad a \leq a' \quad \text{e} \quad b \leq b'$$

(*b*) ***Ordem lexicográfica***: Suponha que S e T são conjuntos linearmente ordenados. Então, a seguir, temos uma relação de ordem no conjunto produto $S \times T$, chamada de *lexicográfica* ou *ordem alfabética*:

$$(a, b) \prec (a', b') \quad \text{se} \quad a < b \quad \text{ou se} \quad a = a' \quad \text{e} \quad b < b'$$

Essa ordem pode ser estendida para $S_1 \times S_2 \times \ldots \times S_n$, como se segue:

$$(a_1, a_2, \ldots, a_n) \prec (a'_1, a'_2, \ldots, a'_n) \quad \text{se} \quad a_i = a'_i \text{ para } i = 1, 2, \ldots, k-1 \text{ e } a_k < a'_k$$

Note que a ordem lexicográfica também é linear.

Fechamento de Kleene e ordem

Seja A um alfabeto (não vazio) linearmente ordenado. Lembre-se de que A^*, chamado de fechamento de Kleene de A, consiste em todas as palavras w em A, e $|w|$ denota o comprimento de w. Então, a seguir, temos as duas relações de ordem em A^*.

(*a*) ***Ordem alfabética (lexicográfica)***: O leitor, sem dúvida, está familiarizado com a ordem afabética usual de A^*. Isto é:

(i) $\lambda \prec w$, onde λ é a palavra vazia, e w é qualquer palavra não vazia.

(ii) Suponha que $u = au'$ e $v = bv'$ são palavras não vazias distintas, onde $a, b \in A$ e u' e $v' \in A^*$. Então

$$u \prec v \quad \text{se} \quad a < b \quad \text{ou} \quad \text{se } a = b \text{ mas } u' \prec v'$$

(*b*) ***Ordem de léxico curto***: Aqui, A^* é ordenado antes por comprimento, em seguida, alfabeticamente. Isto é, para quaisquer palavras distintas u e v em A^*,

$$u \prec v \quad \text{se} \quad |u| < |v| \quad \text{ou se} \quad |u| = |v|, \text{ mas } u \text{ precede } v \text{ alfabeticamente}$$

Por exemplo, "to" precede "and", uma vez que $|\text{to}| = 2$, mas $|\text{and}| = 3$. Contudo, "an" precede "to", uma vez que eles possuem o mesmo comprimento, mas "an" precede "to" alfabeticamente. Essa ordem também é conhecida como ***ordem de semigrupo livre***.

14.3 DIAGRAMAS DE HASSE DE CONJUNTOS PARCIALMENTE ORDENADOS

Seja S um conjunto parcialmente ordenado, e suponha que a e b pertencem a S. Dizemos que a é um *predecessor imediato* de b, ou que b é um *sucessor imediato* de a, ou que b é uma *cobertura* de a, escrito na forma

$$a \ll b$$

se $a < b$, mas nenhum elemento de S está entre a e b, isto é, não existe nenhum elemento c em S tal que $a < c < b$.

Suponha que S seja um conjunto finito parcialmente ordenado. Então a ordem em S é completamente conhecida, uma vez que saibamos todos os pares a, b em S tal que $a \ll b$, isto é, uma vez que saibamos a relação $\ll$ em S. Isso segue do fato de que $x < y$ se, e somente se, $x \ll y$ ou se existirem elementos $a_1, a_2, \ldots, a_m$ em S tais que

$$x \ll a_1 \ll a_2 \ll \cdots \ll a_m \ll y$$

O *diagrama de Hasse* de um conjunto finito parcialmente ordenado S é o grafo orientado cujos vértices são os elementos de S e existe uma aresta orientada de a a b quando $a \ll b$ em S. (Em vez de esboçar uma flecha de a a b, colocamos, às vezes, b acima de a e esboçamos uma linha entre eles. Assim, é entendido que o movimento para cima indica sucessão.) No diagrama criado, existe uma aresta orientada do vértice x ao y se, e somente se, $x \ll y$. Além disso, não podem existir ciclos (orientados) no diagrama de S, uma vez que a relação de ordem é antissimétrica.

O diagrama de Hasse de um conjunto parcialmente ordenado S é uma imagem de S; logo, é muito útil ao descrevermos tipos de elementos em S. Às vezes, definimos um conjunto parcialmente ordenado ao apresentar seu diagrama de Hasse. Observamos que o diagrama de Hasse de um conjunto parcialmente ordenado S não precisa ser conexo.

Observação: O diagrama de Hasse de um conjunto parcialmente ordenado finito S acaba sendo um gráfico livre de ciclos orientados (GLCD), estudados na Seção 9.9. A investigação aqui é independente da anterior. Aqui, consideramos "ordem" em termos de "menor que" ou "maior que", em vez de relações de adjacência orientadas. Logo, existirá sobreposição de conteúdos.

Exemplo 14.3

(a) Seja $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ ordenada pela relação "x divide y". O diagrama de A é dado na Fig. 14-1(a). (Diferentemente de árvores enraizadas, a direção de uma reta no diagrama de um conjunto parcialmente ordenado é sempre para cima.)

(b) Considere $B = \{a, b, c, d, e\}$. O diagrama na Fig. 14-1(b) define uma ordem parcial em B de maneira natural. Isto é, $d \leq b$, $d \leq a$, $e \leq c$, e assim por diante.

(c) O diagrama de um conjunto finito linearmente ordenado, isto é, uma corrente finita, consiste em apenas um caminho. Por exemplo, a Fig. 14-1(c) mostra o diagrama de uma corrente em cinco elementos.

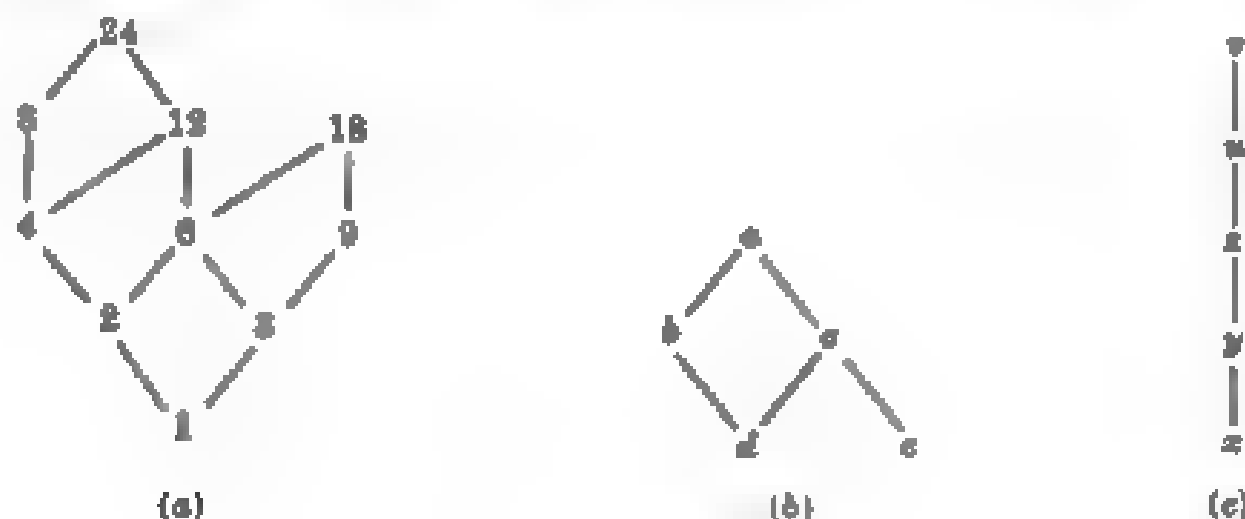



Figura 14-1

Exemplo 14.4 Uma *partição* de um inteiro positivo m é um conjunto de inteiros positivos cuja soma é m. Por exemplo, existem sete partições de $m = 5$, como se segue:

$$5,\quad 3-2,\quad 2-2-1,\quad 1-1-1-1-1,\quad 4-1,\quad 3-1-1,\quad 2-1-1-1$$

Ordenamos as partições de um inteiro m como se segue. Uma partição P_1 precede uma partição P_2 se os inteiros em P_1 podem ser somados para obter os inteiros em P_2 ou, de forma equivalente, se os inteiros em P_2 podem ser subdivididos para obter os inteiros em P_1. Por exemplo,

$$2-2-1 \quad \text{precede} \quad 3-2$$

uma vez que $2 + 1 = 3$. Por outro lado, $3 - 1 - 1$ e $2 - 2 - 1$ são não comparáveis.

A Figura 14-2 resulta no diagrama de Hasse das partições de $m = 5$

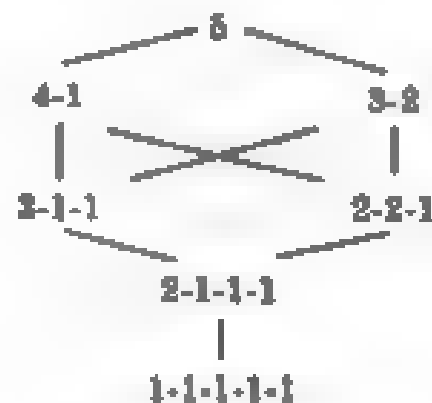



Figura 14-2

Mínimos e máximos, primeiro e último elementos

Seja S um conjunto parcialmente ordenado. Um elemento a em S é chamado de elemento *mínimo* se nenhum elemento de S preceder estritamente (for menor que) a. De forma similar, um elemento b em S é chamado de *máximo* se nenhum elemento de S suceder estritamente (for maior que) b. Geometricamente falando, a é um elemento mínimo se nenhuma aresta entra em a (por baixo) e b é um elemento máximo se nenhuma aresta sai de b (para cima). Notamos que S pode ter mais do que um elemento mínimo e mais do que um máximo.

Se S é infinito, então S pode não ter elementos máximo e mínimo. Por exemplo, o conjunto $\mathbf{Z}$ de inteiros com a ordem usual $<$ não possui elementos mínimo ou máximo. Por outro lado, se S é finito, então S deve ter, ao menos, um elemento mínimo e, ao menos, um elemento máximo.

Um elemento a em S é chamado de *primeiro* elemento se, para todo elemento x em S,

$$a \precsim x$$

isto é, se b sucede todos os outros elementos em S. De forma similar, um elemento b em S é chamado de *último* elemento se, para todo elemento y em S,

$$y \precsim b$$

isto é, se b sucede todos os outros elementos em S. Notamos que S pode ter, no máximo, um primeiro elemento, que deve ser um elemento mínimo, e S pode ter no máximo um último elemento, que deve ser um elemento máximo. Falando de forma geral, S pode não ter um primeiro ou um último elemento, mesmo quando S for finito.

Exemplo 14.5

(a) Considere os três conjuntos parcialmente ordenados no Exemplo 14-3 cujos diagramas de Hasse aparecem na Fig. 14-1.

(i) A possui dois elementos máximos (18 e 24) e nenhum deles é um último elemento. A possui apenas um elemento mínimo (1) que é, também, um primeiro elemento.

(ii) B possui dois elementos mínimos (d e e) e nenhum deles é um primeiro elemento. B possui apenas um elemento máximo (a) que é, também, um último elemento.

(iii) A corrente possui um elemento mínimo (x), que é um primeiro elemento, e um elemento máximo (v), que é um último elemento.

(b) Seja A qualquer conjunto não vazio, e considere $P(A)$ como sendo o conjunto potência de A ordenado por inclusão de conjuntos. Então, o conjunto vazio $\emptyset$ é um primeiro elemento de $P(A)$, uma vez que, para qualquer conjunto X, temos $\emptyset \subseteq X$. Além disso, A é um último elemento de $P(A)$, uma vez que todo elemento Y de $P(A)$ é, por definição, um subconjunto de A, isto é, $Y \subseteq A$.

14.4 ENUMERAÇÃO CONSISTENTE

Suponha que S é um conjunto finito parcialmente ordenado. Frequentemente, queremos associar inteiros positivos aos elementos de S de tal forma que a ordem seja preservada. Isto é, procuramos uma função $f: S \to \mathbf{N}$ de forma que, se $a \prec b$, então $f(a) < f(b)$. Tal função é chamada de *enumeração consistente* de S. O fato de que isso sempre pode ser feito é o conteúdo do teorema a seguir.

Teorema 14.1: Existe uma enumeração consistente para qualquer conjunto parcialmente ordenado finito A.

Demonstramos esse teorema no Problema 14.8. De fato, provamos que, se S possui n elementos, então existe uma enumeração consistente $f: S \to \{1, 2, \ldots, n\}$.

Enfatizamos que tal enumeração não precisa ser única. Por exemplo, a seguir estão duas enumerações para o conjunto parcialmente ordenado da Fig. 14-1(b):

(i) $f(d) = 1, f(e) = 2, f(b) = 3, f(c) = 4, f(a) = 5.$

(ii) $g(e) = 1, g(d) = 2, g(c) = 3, g(b) = 4, g(a) = 5.$

Contudo, a corrente na Fig. 14-1(c) admite apenas uma enumeração consistente se mapearmos o conjunto como $\{1, 2, 3, 4, 5\}$. Especificamente, devemos associar:

$$h(x) = 1, \quad h(y) = 2, \quad h(z) = 3, \quad h(u) = 4, \quad h(v) = 5$$

14.5 SUPREMO E ÍNFIMO

Seja A um subconjunto de um conjunto parcialmente ordenado S. Um elemento M em S é chamado de *limite superior* (ou *cota superior*) de A se M suceder todos os elementos de A, ou seja, para todo x em A, temos

$$x \precsim M$$

Se um limite superior de A precede qualquer outro limite superior de A, então ele é chamado de *supremo* de A e é denotado por

$$\sup(A)$$

Também escrevemos $\sup(a_1, \ldots, a_n)$ em vez de $\sup(A)$ se A consiste nos elementos $a_1, \ldots, a_n$. Enfatizamos que pode existir, no máximo, um $\sup(A)$; contudo, $\sup(A)$ pode não existir.

Analogamente, um elemento m em um conjunto parcialmente ordenado S é chamado de *limite inferior* (ou *cota inferior*) de um subconjunto A de S se m precede todos os outros elementos de A, isto é, se para todo y em A, temos

$$m \precsim y$$

Se um limite inferior de A sucede todos os outros limites inferiores de A, então ele é chamado de *ínfimo* de A e é denotado por

$$\inf(A), \quad \text{ou} \quad \inf(a_1, \ldots, a_n)$$

se A consiste nos elementos $a_1, \ldots, a_n$. Pode existir, no máximo, um $\inf(A)$, mas $\inf(A)$ pode não existir.

Alguns textos usam o termo *menor limite superior* em vez de supremo e, então escrevem lub(A) em vez de sup(A); usam o termo *maior limite inferior* em vez de ínfimo e escrevem glb(A) em vez de inf(A).

Se A possui um limite superior, dizemos que A é *limitado* (*cotado*) *superiormente* e, se A possui um limite inferior, dizemos que A é *limitado* (*cotado*) *inferiormente*. Especificamente, A é *limitado* (*cotado*) se A é limitado superior e inferiormente.

Exemplo 14.6

(a) Seja $S = \{a, b, c, d, e, f\}$ ordenado como mostrado na Fig. 14-3(*a*) e seja $A = \{b, c, d\}$. Os limites superiores de A são e e f, uma vez que apenas e e f sucedem todos os outros elementos em A. Os limites inferiores de A são a e b, uma vez que apenas a e b precedem todos os outros elementos de A. Note que e e f não são comparáveis; logo, $\sup(A)$ não existe. Contudo, b sucede também a; logo, $\inf(A) = b$.

(b) Seja $S = \{1, 2, 3, \ldots, 8\}$ ordenado como é mostrado na Fig. 14-3(*b*) e seja $A = \{4, 5, 7\}$. Os limites superiores de A são 1, 2 e 3 e o único limite inferior é 8. Note que 7 não é um limite inferior, uma vez que 7 não precede 4. Aqui, $\sup(A) = 3$, uma vez que o 3 precede os outros limites superiores 1 e 2. Note que $\inf(A) = 8$, uma vez que 8 é o único limite inferior.

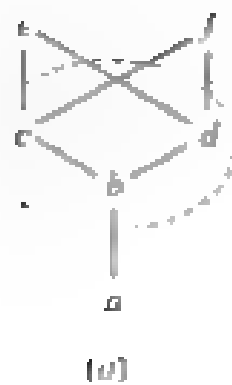
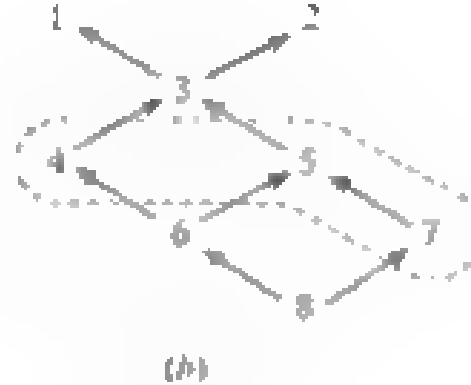
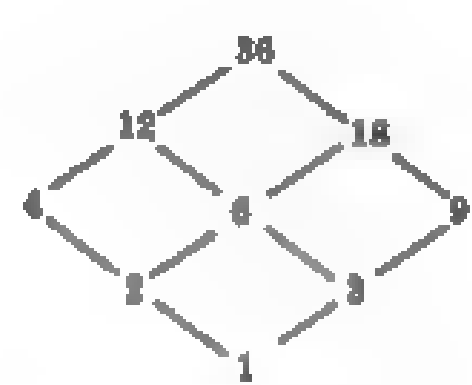



Figura 14-3

Figura 14-4

Em termos gerais, $\sup(a, b)$ e $\inf(a, b)$ não precisam existir para todo par de elementos a e b em um conjunto parcialmente ordenado S. Damos agora dois exemplos de conjuntos parcialmente ordenados onde $\sup(a, b)$ e $\inf(a, b)$ existem para todo a e b no conjunto.

Exemplo 14.7

(a) Seja o conjunto **N** de inteiros positivos ordenado por divisibilidade. O *máximo divisor comum* de a e b em **N**, denotado por

$$\text{mdc}(a, b)$$

é o maior inteiro que divide a e b. O *mínimo múltiplo comum* de a e b, denotado por

$$\text{mmc}(a, b)$$

É o menor inteiro divisível tanto por a quanto por b.

Um teorema importante na teoria dos números determina que todo divisor comum de a e b divide $\text{mdc}(a, b)$. É possível, também, provar que $\text{mmc}(a, b)$ divide todo múltiplo de a e b. Logo,

$$\text{mdc}(a, b) = \inf(a, b) \quad \text{e} \quad \text{mmc}(a, b) = \sup(a, b)$$

Em outras palavras, $\inf(a, b)$ e $\sup(a, b)$ existem para qualquer par de elementos de **N** ordenado por divisibilidade.

(b) Para todo inteiro positivo m, assumiremos que $\mathbf{D}_m$ denota o conjunto de divisores de m ordenado por divisibilidade. O diagrama de Hasse de

$$\mathbf{D}_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

aparece na Fig. 14-4. Novamente, $\inf(a, b) = \text{mdc}(a, b)$ e $\sup(a, b) = \text{mmc}(a, b)$ existem para qualquer par a, b em $\mathbf{D}_m$.

14.6 CONJUNTOS ORDENADOS ISOMORFOS (SIMILARES)

Suponha que X e Y são conjuntos parcialmente ordenados. Uma função um para um (injetora) $f: X \to Y$ é chamada de *mapeamento de similaridade* de X em Y se f preservar a relação de ordem, isto é, se as duas condições a seguir forem válidas para qualquer par a e a' em X:

(1) Se $a \precsim a'$, então $f(a) \precsim f(a')$.

(2) Se $a \parallel a'$ (não comparável), então $f(a) \parallel f(a')$.

Logo, se A e B são linearmente ordenados, então apenas (1) é necessária para f ser um mapeamento de similaridade.

Dois conjuntos ordenados X e Y são ditos *isomorfos* ou *similares*, escrito

$$X \simeq Y$$

se existir uma correspondência um para um (mapeamento bijetor) $f: X \to Y$ que preserva as relações de ordem, isto é, que seja um mapeamento de similaridade.

Exemplo 14.6 Suponha que $X = \{1, 2, 6, 8, 12\}$ é ordenado por divisibilidade, e suponha que $Y = \{a, b, c, d, e\}$ é isomorfo a X; digamos que a função f a seguir é um mapeamento de similaridade de X em Y:

$$f = \{(1, e), (2, d), (6, b), (8, c), (12, a)\}$$

Esboce o diagrama de Hasse de Y.

O mapeamento de similaridade preserva a ordem do conjunto inicial X e é de um para um e sobrejetora. Logo, o mapeamento pode ser visto apenas como uma remarcação dos vértices no diagrama de Hasse do conjunto inicial X. Os diagramas de Hasse tanto para X quanto para Y aparecem na Fig. 14-5.

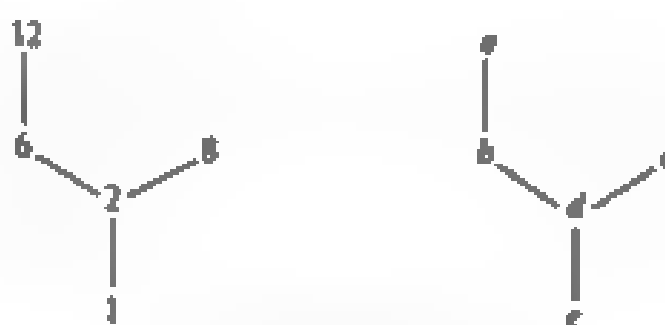



Figura 14-5

14.7 CONJUNTOS BEM-ORDENADOS

Começamos com uma definição.

Definição 14.1: Um conjunto ordenado S é dito *bem-ordenado* se todo subconjunto de S possui um primeiro elemento.

O exemplo clássico de um conjunto bem-ordenado é o conjunto $\mathbf{N}$ de inteiros positivos com a ordem usual $\le$. Os fatos a seguir são consequência direta da definição.

(1) Um conjunto bem-ordenado é linearmente ordenado. Se $a, b, \in S$, então $\{a, b\}$ possui um primeiro elemento, logo, a e b são comparáveis.

(2) Todo subconjunto de um conjunto bem-ordenado é, também, bem-ordenado.

(3) Se X é bem-ordenado e Y é isomorfo a X, então Y é bem-ordenado.

(4) Todos os conjuntos finitos linearmente ordenados com o mesmo número n de elementos são bem-ordenados e são todos isomorfos entre si. Na verdade, eles são todos isomorfos a $\{1, 2, \ldots, n\}$ com a ordem usual $\le$.

(5) Todo elemento $a \in S$ que não seja um último elemento, possui um sucessor imediato. Considere que $M(a)$ denota o conjunto de elementos que sucedem a imediatamente. Então o primeiro elemento de $M(a)$ é o sucessor imediato de a.

Exemplo 14.9

(a) O conjunto **Z** de inteiros com a ordem usual $\leq$ é linearmente ordenado e todo elemento possui um sucessor e predecessor imediatos, mas **Z** não é bem-ordenado. Por exemplo, **Z** não possui primeiro elemento. Contudo, qualquer subconjunto de **Z** que é cotado inferiormente é bem-ordenado.

(b) O conjunto **Q** de números racionais com a ordem usual $<$ é linearmente ordenado, mas nenhum elemento em **Q** possui um sucessor ou predecessor imediato. Se $a, b \in Q$, digamos $a < b$, então $(a + b)/2 \in \mathbf{Q}$ e

$$a < \frac{a+b}{2} < b$$

(c) Considere os conjuntos bem-ordenados disjuntos

$$A = \{1, 3, 5, \ldots\} \text{ e } B = \{2, 4, 6, \ldots\}$$

Então o conjunto ordenado a seguir

$$S = \{A; B\} = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

é bem-ordenado. Note que, fora o primeiro elemento 1, o elemento 2 não possui um predecessor imediato.

Notação: Aqui e subsequentemente, se $A, B, \ldots$ são conjuntos ordenados disjuntos, então $\{A, B, \ldots\}$ refere-se ao conjunto $A \cup B \cup \ldots$ ordenado em relação à posição da esquerda para a direita; isto é, os elementos no mesmo conjunto mantêm sua ordem, e qualquer elemento em um conjunto da esquerda precede qualquer elemento em um conjunto à sua direita. Logo, todo elemento em A precede todo elemento em B, e assim por diante

Indução transfinita

Primeiro, relembremos o Princípio de Indução Matemática (Veja as Seções 1.8 e 11.3.)

Princípio de Indução Matemática: Seja A um subconjunto do conjunto **N** de inteiros positivos com as duas propriedades a seguir:

(i) $1 \in A$.
(ii) Se $k \in A$, então $k + 1 \in A$.

Então $A = \mathbf{N}$.

Os princípios acima referem-se a um dos axiomas de Peano para os números naturais (inteiros positivos) **N**. Existe uma outra forma que é mais conveniente de se usar, dependendo do caso.

Princípio de Indução Matemática (segunda forma): Seja A um subconjunto de **N** com as duas propriedades a seguir:

(i) $1 \in A$.
(ii) Se j pertence a A para $1 \leq j < k$, então $k \in A$.

Então $A = N$

A segunda forma de indução é equivalente ao fato de que **N** é bem-ordenado (Teorema 11.6). Na verdade, existe uma declaração similar que é verdadeira para todo conjunto bem-ordenado.

Princípio de Indução Transfinita: Seja A um subconjunto de um conjunto bem-ordenado S com as duas propriedades a seguir:

(i) $a_0 \in A$.

(ii) Se $s(a) \subseteq A$, então $a \in A$.

Então $A = S$

Aqui a_0 é o primeiro elemento de S e $s(a)$, chamado de *segmento inicial* de a, é definido como sendo o conjunto de todos os elementos de S que imediatamente precedem a.

Axioma da escolha, teorema da boa ordem

Seja $\{A_i : i \in I\}$ uma coleção de conjuntos disjuntos não vazios. Assumimos que cada $A_i \subseteq X$. Uma função $f : \{A_i\} \to X$ é chamada de *função escolha* se $f(A_i) = a_i \in A_i$. Em outras palavras, f "escolhe" um ponto $a_i \in A_i$ para cada conjunto A_i

O axioma da escolha está na fundamentação da matemática e, em particular, da teoria de conjuntos. Esse axioma com "aparência inocente", a seguir, demonstra como consequência um dos mais importantes e poderosos resultados na matemática.

Axioma da escolha: Existe uma função escolha para qualquer coleção não vazia de conjuntos disjuntos não vazios.

Uma das consequências do axioma da escolha é o teorema a seguir, que é atribuído a Zermelo.

Teorema da boa ordem: Todo conjunto S pode ser bem-ordenado.

A demonstração desse teorema está além do objetivo deste texto. Além disso, uma vez que todas as nossas estruturas são finitas ou contáveis, não precisaremos usar esse teorema. Indução matemática básica é o suficiente para nós.

14.8 RETICULADOS

Existem duas maneiras de se definir um reticulado L. Uma das maneiras é definir L em termos de um conjunto parcialmente odenado. Especificamente, um reticulado L pode ser definido como um conjunto parcialmente ordenado em que inf (a, b) e sup (a, b) existem para qualquer par de elementos $a, b \in L$. Outra maneira é definir um reticulado L de forma axiomática. Fazemos isso a seguir

Axiomas definindo um reticulado

Seja L um conjunto não vazio fechado sob duas operações binárias chamadas de *conjunção* e *disjunção*, denotadas, respectivamente, por $\wedge$ e $\vee$. Então L é chamado de *reticulado* se os axiomas a seguir forem válidos, onde a, b e c são elementos em L.

[L_1] Lei Comutativa:
(1a) $a \wedge b = b \wedge a$ (1b) $a \vee b = b \vee a$

[L_2] Lei Associativa:
(2a) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ (2b) $(a \vee b) \vee c = a \vee (b \vee c)$

[L_3] Lei da Absorção:
(3a) $a \wedge (a \vee b) = a$ (3b) $a \vee (a \wedge b) = a$

Às vezes, denotamos o reticulado usando $(L, \wedge, \vee)$, quando queremos mostrar quais operações estão envolvidas.

Lei da dualidade e da idempotência

A *dual* de qualquer afirmação em um reticulado $(L, \wedge, \vee)$ é definida como sendo a afirmação obtida pela permutação de $\wedge$ e $\vee$. Por exemplo, a dual de

$$a \wedge (b \vee a) = a \vee a \quad \text{é} \quad a \vee (b \wedge a) = a \wedge a$$

Note que a dual de cada axioma de um reticulado é, também, um axioma. Logo, o Princípio de Dualidade é válido, isto é:

Teorema 14.2 (Princípio de Dualidade): A dual de qualquer teorema em um reticulado é, também, um teorema.

Isso é consequência do fato de que o teorema da dualidade pode ser demonstrado usando a dualidade de cada passo da demonstração do teorema original.

Uma propriedade importante de reticulados é consequência direta das Leis de Absorção.

Teorema 14.3 (Lei da Idempotência): (i) $a \wedge a = a$, (ii) $a \vee a = a$.

A demonstração de (i) necessita de apenas duas linhas.

$$\begin{aligned} a \wedge a &= a \wedge (a \vee (a \wedge b)) \qquad \text{(usando (3}b\text{))} \\ &= a \qquad \text{(usando (3}a\text{))} \end{aligned}$$

A demonstração de (ii) segue do Princípio de Dualidade acima (ou pode ser provado de maneira similar).

Reticulados e ordem

Dado um reticulado L, podemos definir uma ordem parcial em L, como se segue.

$$a \precsim b \quad \text{se} \quad a \wedge b = a$$

Analogamente, podemos definir

$$a \precsim b \quad \text{se} \quad a \vee b = b$$

Colocamos esses resultados em um teorema.

Teorema 14.4: Seja L um reticulado. Então:

(i) $a \wedge b = a$ se, e somente se, if $a \vee b = b$.
(ii) A relação $a \precsim b$ (definida por $a \wedge b = a$ ou $a \vee b = b$) é uma ordem parcial em L.

Agora que temos uma ordem parcial em qualquer reticulado L, podemos imaginar L como um diagrama, como foi feito para conjuntos parcialmente ordenados em geral.

Exemplo 14.10 Seja C uma coleção de conjuntos fechados sob interseção e união. Então $(C, \cap, \cup)$ é um reticulado. Nesse reticulado, as relações de ordem parcial são as mesmas que na relação de inclusão de conjuntos. A Figura 14-6 mostra o diagrama do reticulado L de todos os subconjuntos de $\{a, b, c\}$

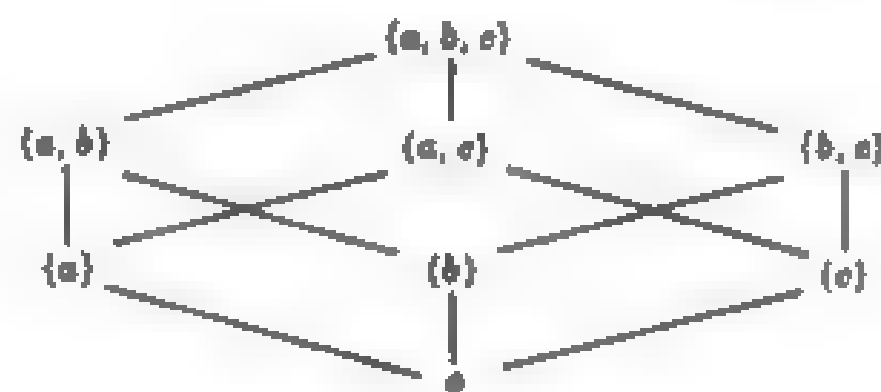



Figura 14-6

Mostramos aqui como definir uma ordem parcial em um reticulado L. O próximo teorema nos diz quando podemos definir um reticulado em um conjunto parcialmente ordenado P de tal forma que o reticulado nos dará a ordem original em P.

Teorema 14.5: Seja P um conjunto parcialmente ordenado tal que inf (a, b) e sup (a, b) existam para qualquer a, b em P. Fazendo

$$a \wedge b = \inf(a, b) \quad \text{e} \quad a \vee b = \sup(a, b)$$

temos que $(P, \wedge, \vee)$ é um reticulado. Além disso, a ordem parcial em P induzida pelo reticulado é a mesma ordem parcial original em P.

A recíproca do teorma acima também é verdadeira. Isto é, seja L um reticulado e $\precsim$ a ordem parcial induzida em L. Então inf (a, b) e sup (a, b) existem para qualquer par a, b em L, e o reticulado obtido a partir do conjunto parcialmente ordenado $(L, \precsim)$ é o reticulado original. Logo, temos o seguinte:

Definição Alternativa: Um reticulado é um conjunto parcialmente ordenado em que

$$a \wedge b = \inf(a, b) \quad \text{e} \quad a \vee b = \sup(a, b)$$

existem para qualquer par de elementos a e b.

Notamos, em primeiro lugar, que qualquer conjunto linearmente ordenado é um reticulado, uma vez que inf $(a, b) = a$ e sup $(a, b) = b$ quando $a \precsim b$. Segundo o Exemplo 14.7, os inteiros positivos **N** e o conjunto $\mathbf{D}_m$ de divisores de m são reticulados sob a relação de divisibilidade.

Subreticulados, reticulados isomorfos

Suponha que M é um subconjunto não vazio de um reticulado L. Dizemos que M é um subreticulado de L se M em si for um reticulado também (em relação às operações de L). Notamos que M é um subreticulado de L se, e somente se, M for fechado sob as operações de $\wedge$ e $\vee$ de L. Por exemplo, o conjunto $\mathbf{D}_m$ de divisores de m é um subreticulado dos inteiros positivos **N** sob divisibilidade.

Dois reticulados L e L' são *isomorfos* se existir uma correspondência de um para um $f: L \to L'$ tal que

$$f(a \wedge b) = f(a) \wedge f(b) \quad \text{e} \quad f(a \vee b) = f(a) \vee f(b)$$

para quaisquer elementos a, b em L.

14.9 RETICULADOS COTADOS

Um reticulado L é considerado como tendo um *limite inferior* 0 se, para qualquer elemento x em L, temos $0 \precsim x$. Analogamente, L tem um *limite superior* I se, para qualquer x em L, temos $x \precsim I$. Dizemos que L é *delimitado* (*cotado*) se L possui tanto o limite inferior 0 quanto o limite superior I. Em tal reticulado, temos as identidades

$$a \vee I = I, \quad a \wedge I = a, \quad a \vee 0 = a, \quad a \wedge 0 = 0$$

para qualquer elemento a em L.

Os inteiros não negativos com a ordem usual,

$$0 < 1 < 2 < 3 < 4 < \cdots$$

possuem 0 como o limite inferior, mas não possuem o limite superior. Por outro lado, o reticulado $P(U)$ de todos os subconjuntos de qualquer conjunto universal **U** é um reticulado cotado com **U** como seu limite superior e Ø como limite inferior.

Suponha que $L = \{a_1, a_2, \ldots, a_n\}$ é um reticulado finito. Então

$$a_1 \vee a_2 \vee \cdots \vee a_n \quad \text{e} \quad a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

são limites superior e inferior para L, respectivamente. Logo, temos

Teorema 14.6: Todo reticulado L finito é cotado.

14.10 RETICULADOS DISTRIBUTIVOS

Um reticulado L é dito *distributivo* se, para quaisquer elementos a, b e c em L, temos o seguinte:
[L_4] Lei Distributiva:

$$(4a)\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \qquad (4b)\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Caso contrário, L é dito *não distributivo*. Notamos que, segundo o Princípio de Dualidade, a condição (4a) é válida se, e somente se, (4b) também o for.

A Figura 14.7(a) é um reticulado não distributivo, uma vez que

$$a \vee (b \wedge c) = a \vee 0 = a, \quad \text{mas} \quad (a \vee b) \wedge (a \vee c) = I \wedge c = c$$

A Figura 14-7(b) é, também, um reticulado não distributivo. Na verdade, temos a seguinte caracterização de tais reticulados.

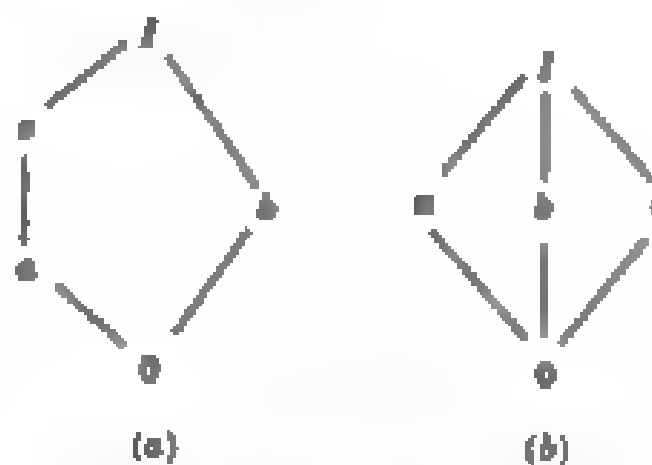



Figura 14-7

Teorema 14.7: Um reticulado L é não distributivo se, e somente se, ele contém um subreticulado isomorfo à Fig 14-7(a) ou à Fig. 14-7(b).

A demonstração desse teorema está além do objetivo deste texto.

União de elementos irredutíveis, átomos

Seja L um reticulado com limite inferior 0. Um elemento a em L é dito uma *união irredutível* se $a = x \vee y$ implica $a = x$ ou $a = y$. (Números primos sob multiplicação possuem essa propriedade, isto é, se $p = ab$, então $p = a$ ou $p = b$, onde p é primo.) Claramente, 0 é uma união irredutível. Se a possui pelo menos dois predecessores imediatos, digamos b_1 e b_2, como na Fig. 14-8(a), então $a = b_1 \vee b_2$ e, portanto, a não é uma união irredutível. Por outro lado, se a possui um único predecessor imediato c, então $a \neq \sup(b_1, b_2) = b_1 \vee b_2$ para quaisquer outros elementos b_1 e b_2, pois c estaria entre os b's e o a, como mostrado na Fig. 14-8(b). Em outras palavras, $a \neq 0$ é uma união irredutível se, e somente se, a possuir um único predecessor imediato. Os elementos que sucedem imediatamente o 0, chamados de *átomos*, são uniões irredutíveis. Contudo, os reticulados podem ter outros elementos que são uniões irredutíveis. Por exemplo, o elemento c na Fig. 14-7(a) não é um átomo, mas é uma união irredutível, uma vez que a é seu único predecessor imediato.

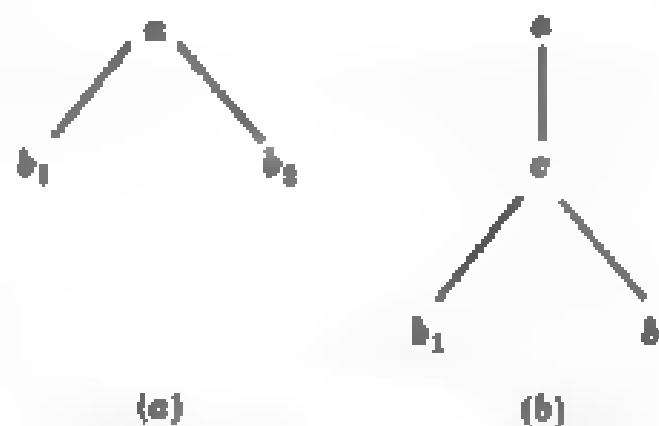



Figura 14-8

Se um elemento a em um reticulado L finito não é uma união irredutível, então podemos escrever $a = b_1 \vee b_2$. Logo, podemos escrever também b_1 e b_2 como a união de outros elementos se eles não são uniões irredutíveis; e assim por diante. Uma vez que L é finito, finalmente temos

$$a = d_1 \vee d_2 \vee \cdots \vee d_n$$

onde os d's são uniões irredutíveis. Se d_i precede d_j, então $d_i \vee d_j = d_j$; assim, podemos deletar o d_i da expressão. Em outras palavras, podemos assumir que os d's são *não redundantes*, ou seja, nenhum d precede qualquer outro d. Enfatizamos que tal expressão não precisa ser única, por exemplo, $I = a \vee b$ e $I = b \vee c$ em ambos os reticulados na Fig. 14-7. Agora enunciamos o principal teorema desta seção (demonstrado no Problema 14.28).

Teorema 14.8: Seja L um reticulado distributivo finito. Então todo a em L pode ser escrito de forma única (exceto pela sua ordem) como a união das uniões não redundantes de elementos irredutíveis.

Na verdade, esse teorema pode ser generalizado para reticulados com *comprimento finito*, isto é, onde todos os subconjuntos linearmente ordenados são finitos. (O Problema 14.30 nos dá um reticulado infinito com comprimento finito.)

14.11 COMPLEMENTARES, RETICULADOS COMPLEMENTADOS

Seja L um reticulado cotado com limite inferior 0 e limite superior I. Seja a um elemento de L. Um elemento x em L é chamado de *complementar* de a se

$$a \vee x = I \quad \text{e} \quad a \wedge x = 0$$

Complementares não precisam existir nem ser únicos. Por exemplo, os elementos a e c são, ambos, complementares de b na Fig. 14-7(a). Além disso, os elementos y, z e u na corrente da Fig. 14-1 não possuem complementares. Temos o resultado a seguir.

Teorema 14.9: Seja L um reticulado distributivo cotado. Então os complementares serão únicos, caso existam.

Demonstração: Suponha que x e y são complementares de qualquer elemento a em L. Então

$$a \vee x = I, \quad a \vee y = I, \quad a \wedge x = 0, \quad a \wedge y = 0$$

Usando a propriedade distributiva,

$$x = x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = I \wedge (x \vee y) = x \vee y$$

Similarmente,

$$y = y \vee 0 = y \vee (a \wedge x) = (y \vee a) \wedge (y \vee x) = I \wedge (y \vee x) = y \vee x$$

Logo,

$$x = x \vee y = y \vee x = y$$

e o teorema está demonstrado.

Reticulados complementados

Um reticulado L é dito *complementado* se L é cotado e todo elemento nele possui um complementar. A Figura 14-7(b) mostra um reticulado complementado onde os complementares não são únicos. Por outro lado, o reticulado $P(\mathrm{U})$ de todos os subconjuntos de um conjunto universo U é complementado, e cada subconjunto A de U possui o complementar único $A^C = \mathrm{U} \backslash A$.

Teorema 14.10: Seja L um reticulado complementado com complementares únicos. Então, os elementos de união irredutível de L, além de 0, são seus átomos.

Combinando esse teorema com o Teorema 14.8 e o 14.9, temos um resultado importante.

Teorema 14.11: Seja L um reticulado distributivo complementado. Então todo elemento a em L é a união de um conjunto único de átomos.

Observação: Alguns textos definem um reticulado L como sendo complementado se cada a em L possui um complementar único. O Teorema 14 10 é, nesses textos, enunciado de maneira diferente.

Problemas Resolvidos

Conjuntos ordenados e subconjuntos

14.1 Seja $\mathbf{N} = \{1, 2, 3, \ldots\}$ ordenado por divisibilidade. Determine se cada um dos seguintes subconjuntos de $\mathbf{N}$ é linearmente (totalmente) ordenado.

(*a*) $\{24, 2, 6\}$; (*c*) $\mathbf{N} = \{1, 2, 3 \ldots\}$; (*e*) $\{7\}$;

(*b*) $\{3, 15, 5\}$; (*d*) $\{2, 8, 32, 4\}$; (*f*) $\{15, 5, 30\}$.

(*a*) Uma vez que 2 divide 6, que divide 24, o conjunto é linearmente ordenado.

(*b*) Uma vez que 3 e 5 não são comparáveis, o conjunto não é linearmente ordenado.

(*c*) Uma vez que 2 e 3 não são comparáveis, o conjunto não é linearmente ordenado.

(*d*) Esse conjunto é linarmente ordenado, uma vez que $2 \prec 4 \prec 8 \prec 32$.

(*e*) Qualquer conjunto que consista em um elemento é linearmente ordenado.

(*f*) Uma vez que 5 divide 15, que divide 30, o conjunto é linearmente ordenado.

14.2 Seja $A = \{1, 2, 3, 4, 5\}$ ordenado pelo diagrama de Hasse na Fig. 14-9(*a*).

(*a*) Insira o símbolo correto, $\prec$, $\succ$ ou $\|$ (não comparável), entre cada par de elementos.

(i) 1___5; (ii) 2___3; (iii) 4___1; (iv) 3___4.

(*b*) Encontre todos os elementos mínimos e máximos de A.

(*c*) A possui um primeiro elemento ou um último?

(*d*) Seja $L(A)$ a notação da coleção de todos os subconjuntos linearmente ordenados de A com 2 ou mais elementos, e considere também que $L(A)$ é ordenado por inclusão de conjuntos. Esboce o diagrama de Hasse de $L(A)$.

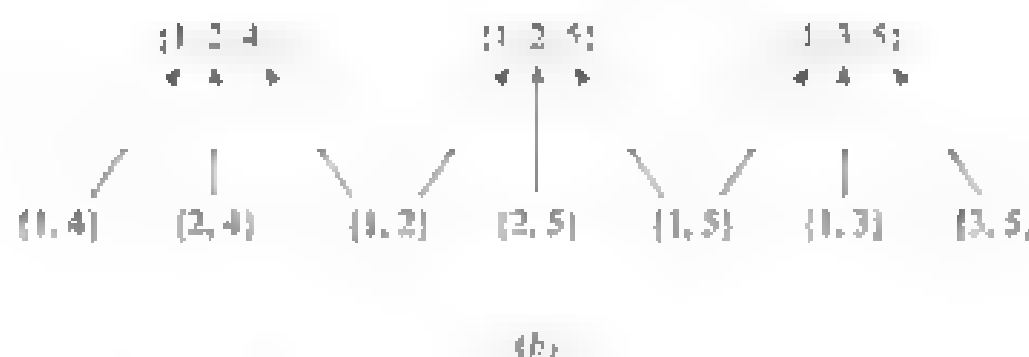
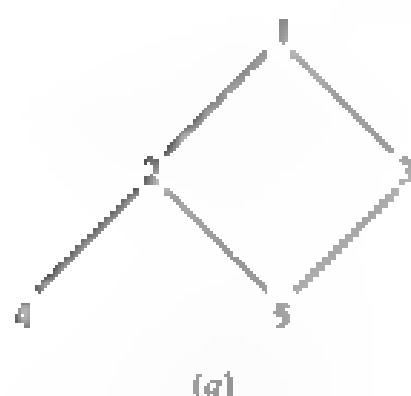



Figura 14-9

(*a*) (i) Uma vez que existe um "caminho" (arestas para cima) de 5 a 3 a 1, 5 precede 1, logo $1 \succ 5$.

(ii) Não existe um caminho de 2 a 3 ou vice-versa, logo, $2 \| 3$.

(iii) Existe um caminho de 4 a 2 a 1, logo, $4 \prec 1$.

(iv) Nem $3 \prec 4$, nem $4 \prec 3$, logo, $3 \| 4$.

(*b*) Nenhum elemento precede imediatamente 4 ou 5, então 4 e 5 são elementos mínimos de A. Nenhum elemento sucede imediatamente 1, então 1 é um elemento máximo de A.

(*c*) A não possui um primeiro elemento. Apesar de 4 e 5 serem elementos mínimos de A, nenhum precede o outro. Contudo, 1 é um último elemento de A, uma vez que 1 sucede todos os elementos de A.

(*d*) Os elementos de $L(A)$ são os seguintes:

$$\{1, 2, 4\},\quad \{1, 2, 5\},\quad \{1, 3, 5\},\quad \{1, 2\},\quad \{1, 4\},\quad \{1, 3\},\quad \{1, 5\},\quad \{2, 4\},\quad \{2, 5\},\quad \{3, 5\}$$

(Note que $\{2, 5\}$ e $\{3, 4\}$ não são linearmente ordenados.) O diagrama de $L(A)$ aparece na Fig. 14-9(*b*).

14.3 Pré-requisitos em uma faculdade é uma familiar ordem parcial de disciplinas disponíveis. Escrevemos $A \prec B$ se a disciplina A é um pré-requisito para B. Considere que C é o conjunto ordenado que consiste nas disciplinas de matemática e seus pré-requisitos são os que aparecem na Fig. 14-10(*a*).

(*a*) Esboce o diagrama de Hasse para a ordem parcial C dessas disciplinas.

(*b*) Encontre os elementos mínimo e máximo de C.

(*c*) C possui um primeiro ou último elemento?

Disciplina	**Pré-requisitos**
Mat. 101	Nenhum
Mat. 201	Mat. 101
Mat. 250	Mat. 101
Mat. 251	Mat. 250
Mat. 340	Mat. 201
Mat. 341	Mat. 340
Mat. 450	Mat. 201, Mat. 250
Mat. 500	Mat. 450, Mat. 251

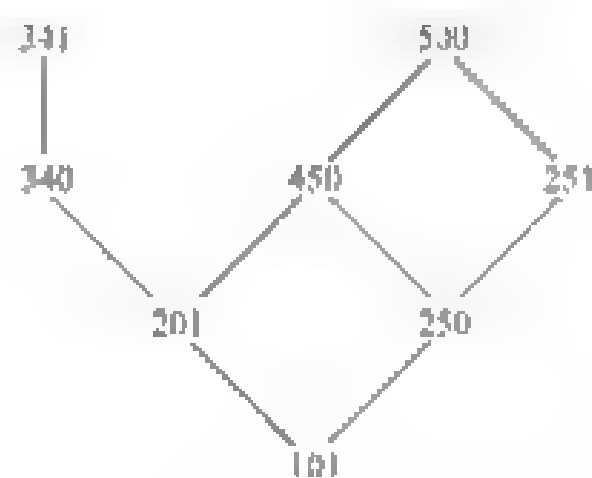
(*a*)

(*b*)

Figura 14-10

(*a*) Mat. 101 deve estar na base do diagrama, uma vez que é a única disciplina para a qual não existe pré-requisito algum. Já que Mat. 201 e Mat. 250 exigem apenas Mat. 101, temos $\ll$ e $\ll$; logo, esboce uma linha inclinada para cima de Mat. 101 até Mat. 201 e outra de Mat. 101 até Mat. 250. Continuando com esse processo, obtemos o diagrama de Hasse na Fig. 14-10(*b*).

(*b*) Nenhum elemento precede imediatamente Mat. 101, então ele é um elemento mínimo de C. Nenhum elemento sucede imediatamente Mat. 341 ou Mat. 500, então cada um deles é um elemento máximo de C.

(*c*) Mat. 101 é um primeiro elemento de C, uma vez que precede qualquer outro elemento do conjunto. Contudo, C não possui último elemento. Apesar de Mat. 341 e Mat. 500 serem elementos máximos, nenhum deles é o último elemento, uma vez que nenhum dos dois precede o outro.

Conjuntos produto e ordem

14.4 Suponha que $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$ é munido da ordem de produto (Seção 14.2) onde $\mathbf{N}$ possui a ordem usual $\leq$.

Insira o símbolo correto, $\prec$, $\succ$ ou $\|$ (não comparável), entre cada um dos seguintes pares de elementos de $\mathbf{N} \times \mathbf{N}$

(*a*) (5, 7) ___ (7, 1); (*c*) (5, 5) ___ (4, 8); (*e*) (7, 9) ___ (4, 1);

(*b*) (4, 6) ___ (4, 2); (*d*) (1, 3) ___ (1, 7); (*f*) (7, 9) ___ (8, 2).

Aqui, $(a, b) \prec (a', b')$ se $a \leq a'$ e $b \leq b'$ ou se $a < a'$ e $b < b'$. Logo

(*a*) $\|$ uma vez que $5 < 7$, mas $7 > 1$. (*c*) $\|$ uma vez que $5 > 4$ e $5 < 8$. (*e*) $\succ$ uma vez que $7 > 4$ e $9 > 1$.

(*b*) $\succ$ uma vez que $4 = 4$ e $6 > 2$. (*d*) $\prec$ uma vez que $1 = 1$ e $3 < 7$. (*f*) $\|$ uma vez que $7 < 8$ e $9 > 2$.

14.5 Repita o Problema 14.4, usando a ordem lexicográfica de $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$.

Aqui, $(a, b) \prec (a', b')$ se $a < a'$ ou se $a = a'$, mas $b < b'$. Logo:

(*a*) $\prec$ uma vez que $5 < 7$. (*c*) $\succ$ uma vez que $5 > 4$. (*e*) $\succ$ uma vez que $7 > 4$.

(*b*) $\succ$ uma vez que $4 = 4$ e $6 > 2$. (*d*) $\prec$ uma vez que $1 = 1$, mas $3 < 7$. (*f*) $\prec$ uma vez que $7 < 8$.

14.6 Considere o alfabeto da língua inglesa $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ com sua ordem usual (alfabética). (Lembre-se de que $\mathbf{A}^*$ consiste em todas as palavras em $\mathbf{A}$.) Considere a seguinte lista de palavras em $\mathbf{A}^*$

went, forget, to, medicine, me, toast, melt, for, we, arm

(*a*) Organize a lista de palavras usando a ordem *short-lex* (semigrupo livre)

(*b*) Organize a lista de palavras usando a ordem usual (alfabética) de $\mathbf{A}^*$.

(*a*) Primeiro ordene os elementos por comprimento e então lexicograficamente (alfabeticamente):

me, to, we, arm, for, melt, went, toast, forget, medicine

(*b*) A ordem usual (alfabética) implica.

arm, for, forget, me, medicine, melt, to, toast, we, went

Enumerações consistentes

14.7 Suponha que uma estudante queira fazer todos as oito disciplinas de matemática do Problema 14.3, mas apenas uma por semestre.

(*a*) Qual escolha, ou escolhas, ela tem para o primeiro e para o último (oitavo) semestre?

(*b*) Suponha que ela queira cursar Mat. 250 no seu primeiro ano (primeiro ou segundo semestre) e Mat. 340 no seu quarto ano (sétimo ou oitavo semestre). Encontre todas as maneiras com as quais ela pode cursar as oito disciplinas.

(*a*) Segundo a Fig. 14-10, Mat. 101 é o único elemento mínimo e, portanto, deve ser cursada no primeiro semestre. Mat 341 e 500 são ambas elementos máximos e, portanto, qualquer uma delas pode ser cursada no último semestre.

(*b*) Mat 250 não é um elemento mínimo e, portanto, deve ser cursada no segundo semestre Mat 340 não é um elemento máximo, então deve ser cursada no sétimo semestre e Mat. 341 no oitavo semestre. Além disso, Mat. 500 deve ser cursada no sexto semestre. A seguir temos as três possíveis maneiras para cursar as oito disciplinas.

101, 250, 251, 201, 450, 500, 340, 341, 101, 250, 201, 251, 450, 500, 340, 341,

101, 250, 201, 450, 251, 500, 340, 341

14.8 Demonstre o Teorema 14.1. Suponha que S é um conjunto parcialmente ordenado finito com n elementos. Então existe uma enumeração consistente $f: S \to \{1, 2, \ldots, n\}$.

A demonstração é feita por indução sobre o número n de elementos em S. Suponha que $n = 1$, digamos $S = \{s\}$ Então $f(s) = 1$ é uma enumeração consistente de S Agora suponha que $n > 1$ e que o teorema é válido para conjuntos parcialmente ordenados com menos de n elementos. Seja $a \in S$ um elemento mínimo. (Tal elemento a existe, uma vez que S é finito.) Seja $T = S \setminus \{a\}$, então T é um conjunto parcialmente ordenado finito com $n - 1$ elementos e, portanto, por indução, T admite uma enumeração consistente, digamos, $g: T \to \{1, 2, \ldots, n-1\}$ Defina $f: S \to \{1, 2, \ldots, n\}$ por

$$f(x) = \begin{cases} 1, & \text{se } x = a \\ g(x) + 1 & \text{se } x \neq a \end{cases}$$

Então f é a enumeração consistente pedida.

Limites superior e inferior, supremo e ínfimo

14.9 Seja $S = \{a, b, c, d, e, f, g\}$ ordenado como na Fig. 14-11(*a*), e considere que $X = \{c, d, e\}$

(*a*) Encontre os limites superior e inferior de X.

(*b*) Identifique sup (X), o supremo de X, e inf (X), o ínfimo de X, se qualquer um deles existir.

(*a*) Os elementos e, f e g sucedem todos os elementos de X; portanto, e, f e g são os limites superiores de X. O elemento a precede todos os elementos de X, logo, a é o limite inferior de X Note que b não é um limite inferior, uma vez que b não precede c; na verdade, b e c não são comparáveis.

(*b*) Uma vez que e precede f e g, temos $e = \sup(X)$. Da mesma maneira, uma vez que a precede (trivialmente) todo limite inferior de X, temos $a = \inf(X)$. Note que sup (X) pertence a X, mas inf (X) não pertence

14.10 Seja $S = \{1, 2, 3, \ldots, 8\}$ ordenado como na Fig. 14-11(*b*) e $A = \{2, 3, 6\}$.

(*a*) Encontre os limites superior e inferior de A. (*b*) Identifique sup (A) e inf (A), se qualquer um deles existir.

(*a*) O limite superior é 2 e os limites inferiores são 6 e 8.

(*b*) Aqui sup $(A) = 2$ e inf $(A) = 6$.

(a)

(b)

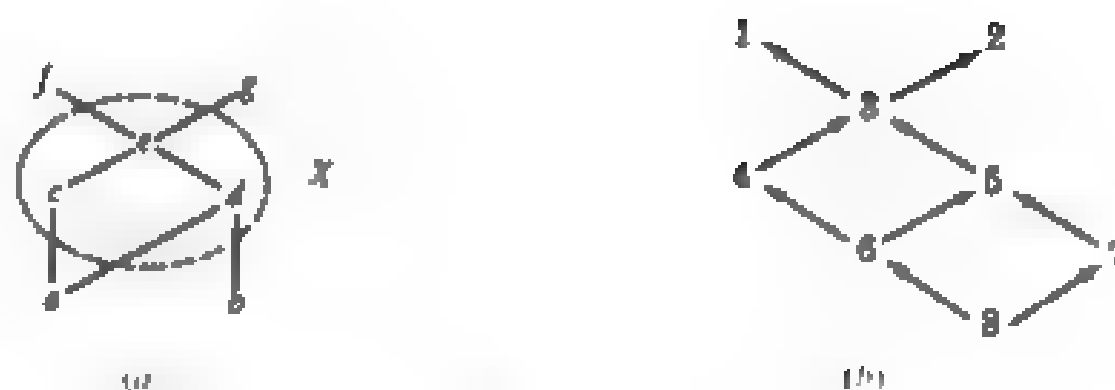



Figura 14-11

14.11 Repita o Problema 14.10 para o subconjunto $B = \{1, 2, 5\}$

(a) Não existe limite superior para B, uma vez que nenhum elemento sucede 1 e 2. Os limites inferiores são 6, 7 e 8.

(b) Trivialmente, sup (A) não existe, uma vez que não existem limites superiores. Apesar de A possuir três limites inferiores, inf (A) não existe, uma vez que nenhum limite sucede 6 e 7.

14.12 Considere o conjunto **Q** de números racionais com a ordem usual $\leq$. Considere o subconjunto D de **Q** definido por

$$D = \{x \mid x \in \mathbf{Q} \quad \text{e} \quad 8 < x^3 < 15\}$$

(a) D é cotado superior ou inferiormente? (b) sup (D) ou inf (D) existem?

(a) O subconjunto D é delimitado tanto superior quanto inferiormente. Por exemplo, 1 é um limite inferior e 100 é um limite superior.

(b) Dizemos que sup (D) não existe. Suponha o caso contrário, em que sup $(D) = x$. Uma vez que $\sqrt{15}$ é irracional, $x > \sqrt{15}$. Contudo, existe um número racional y tal que $\sqrt{15} < y < x$. Logo, y é, também, um limite superior para D. Isso contradiz a constatação de que $x = \sup(D)$. Por outro lado, inf (D) não existe. Especificamente, inf $(D) = 2$.

Conjuntos isomorfos (similares), mapeamento de similaridades

14.13 Suponha que um conjunto parcialmente ordenado A é isomorfo (similar) a um conjunto parcialmente ordenado B e $f: A \to B$ é um mapeamento de similaridade. As declarações a seguir são verdadeiras ou falsas?

(a) Um elemento $a \in A$ é um primeiro (último, mínimo ou máximo) elemento de A se, e somente se, $f(a)$ é um primeiro (último, mínimo ou máximo) elemento de B.

(b) Um elemento $a \in A$ precede imediatamente um elemento $a' \in A$, isto é, $a \ll a'$ se, e somente se, $f(a) \ll f(a')$.

(c) Um elemento $a \in A$ possui r sucessores imediatos em A se, e somente se, $f(a)$ possui r sucessores imediatos em B.

Todas as declarações são verdadeiras, a estrutura de ordem de A é a mesma estrutura de ordem de B.

14.14 Seja $S = \{a, b, c, d, e\}$ o conjunto ordenado na Fig. 14-12(a). Suponha que $A = \{1, 2, 3, 4, 5\}$ é isomorfo a S. Esboce o diagrama de Hasse de A se a seguir está um mapeamento de S para A.

$$f = \{(a, 1), (b, 3), (c, 5), (d, 2), (e, 4)\}$$

O mapeamento de similaridade f preserva a estrutura de ordem de S e, portanto, f pode ser visto apenas como uma remarcação dos vértices do diagrama de S. Logo, a Fig. 14-12(b) mostra o diagrama de Hasse de A.

14.15 Seja $A = \{1, 2, 3, 4, 5\}$ ordenado como na Fig. 14-12(b). Encontre o número n de mapeamentos de similaridade $f: A \to A$.

Uma vez que 1 é o único elemento mínimo de A, e 4 é o único elemento máximo, devemos ter $f(1) = 1$ e $f(4) = 4$. Além disso, $f(3) = 3$, uma vez que 3 é o único sucesor imediato de 1. Por outro lado, existem duas possibilidades para $f(2)$ e $f(5)$, isto é, podemos ter $f(2) = 2$ e $f(5) = 5$ ou $f(2) = 5$ e $f(5) = 2$. Logo, $n = 2$.

14.16 Apresente um exemplo de um conjunto finito não linearmente ordenado $X = (A, R)$ que seja isomorfo a $Y = (A, R^{-1})$, o conjunto A com a ordem inversa.

Seja R a ordenação parcial de $A = \{a, b, c, d, e\}$ desenhada na Fig. 14-13(a).

Então a Fig. 14-13(b) mostra A com a ordem inversa R (O diagrama de R está simplesmente virado de cabeça para baixo para obtermos R^{-1}.) Note que os dois diagramas são idênticos, exceto pelas suas marcações. Logo, X é isomorfo a Y

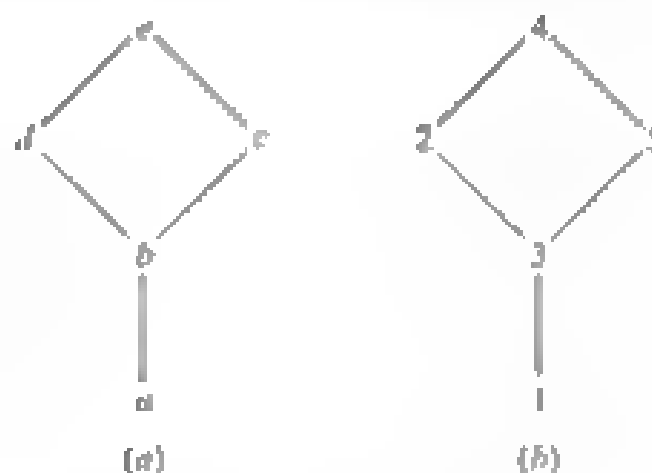



Figura 14-12

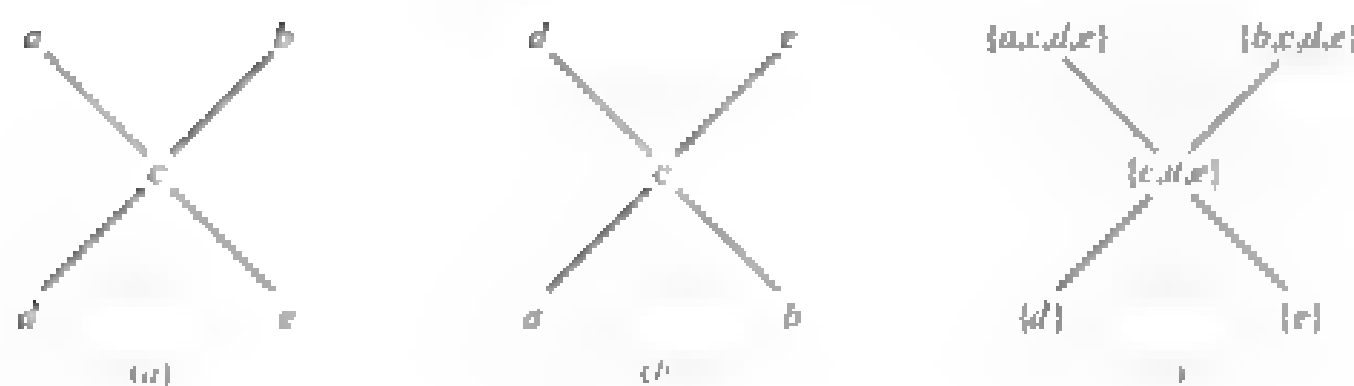



Figura 14-13

14.17 Seja A um conjunto ordenado e, para cada $a \in A$, considere que $p(a)$ denota o conjunto de predecessores de a:

$$p(a) = \{x \mid x \precsim a\}$$

(chamado de *conjunto predecessor* de a). Considere que $p(A)$ denota a coleção de todos os conjuntos predecessores dos elementos em A ordenados por inclusão de conjuntos.

(a) Mostre que A e $p(A)$ são isomorfos ao mostrar que o mapa $f: A \to p(A)$, definido por $f(a) = p(a)$, é um mapeamento de similaridade de A em $p(A)$.

(b) Encontre o diagrama de Hasse de $p(A)$ para o conjunto A na Fig. 14-13(a).

(a) Primeiro mostramos que f preserva a relação de ordem de A. Suponha que $a \precsim b$. Seja $x \in p(a)$. Então $x \precsim a$ e, portanto, $a \precsim b$; logo, $x \in p(b)$. Então, $p(a) \subset p(b)$. Suponha que $a \parallel b$ (não comparável). Então $a \in p(a)$, mas $a \notin p(b)$; logo, $p(a) \not\subseteq p(b)$. De forma similar, $b \in p(b)$, mas $b \notin p(a)$; logo, $p(b) \not\subseteq p(a)$. Portanto, $p(a) \parallel p(b)$. Então f preserva a ordem.

Agora precisamos mostrar que f é um para um e sobrejetora. Suponha que $y \in p(A)$. Então $y = p(a)$ para algum $a \in A$. Logo, $f(a) = p(a) = y$ de forma que f é sobrejetora $p(A)$. Suponha que $a \neq b$. Então $a \prec b$, $b \prec a$ ou $a \parallel b$. No primeiro e terceiro casos, $b \in p(b)$, mas $b \notin p(a)$, e, no segundo caso, $a \in p(a)$, mas $a \notin p(b)$. Consequentemente, nos três casos, temos $p(a) \neq p(b)$. Portanto, f é um para um.

Consequentemente, f é um mapeamento de similaridade de A em $p(A)$ e, então, $A \simeq p(A)$.

(b) Os elementos de $p(A)$ são os que se seguem.

$$p(a) = \{a, c, d, e\}, \quad p(b) = \{b, c, d, e\}, \quad p(c) = \{c, d, e\}, \quad p(d) = \{d\}, \quad p(e) = \{e\}$$

A Figura 14-13(c) nos dá o diagrama de $p(A)$ ordenado por inclusão de conjuntos. Observe que os diagramas na Fig. 14-13(a) e (c) são idênticos, exceto pela demarcação dos vértices.

Conjuntos bem-ordenados

14.18 Prove o Princípio de Indução Transfinita: Seja A um subconjunto de um conjunto bem-ordenado S, com as duas propriedades a seguir: (i) $a_0 \in A$. (ii) Se $s(a) \subseteq A$ então $a \in A$. Portanto $A = S$.

(Aqui a_0 é o primeiro elemento de A e $s(a)$ é o segmento inicial de a, ou seja, o conjunto de todos os elementos precedendo imediatamente a.) Suponha que $A \neq S$. Seja $B = S \setminus A$. Então $B \neq \emptyset$. Uma vez que S é bem-ordenado, B

possui um primeiro elemento b_0. Cada elemento $x \in s(b_0)$ precede b_0 e, portanto, não pertence a B. Logo, todo $x \in s(b_0)$ pertence a A, assim, $s(b_0) \subseteq A$. Segundo (ii), $b_0 \in A$. Isso contradiz o pressuposto de que $b_0 \in S \backslash A$. Logo, o pressuposto original de que $A \neq S$ não é verdadeiro. Portanto, $A = S$.

14.19 Seja S um conjunto bem-ordenado com primeiro elemento a_0. Defina um *elemento limite* de S.

Um elemento $b \in S$ é um elemento limite se $b \neq a_0$ e b não possui predecessor imediato.

14.20 Considere o conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ de inteiros positivos. Todo número em $\mathbf{N}$ pode ser escrito unicamente como um produto de uma potência não negativa de 2 multiplicado por um número ímpar. Suponha que $a, a' \in \mathbf{N}$ e

$$a = 2^r(2s+1) \text{ e } a' = 2^{r'}(2s'+1)$$

onde r, r' e s, s' são inteiros não negativos. Defina:

$$a \prec a' \quad \text{se} \quad r < r' \quad \text{ou} \quad \text{se} \quad r = r', \text{mas } s < s'.$$

(*a*) Insira o símbolo correto, $\prec$ ou $\succ$, entre cada par de números.

(i) 5__14; (ii) 6__9; (iii) 3__20; (iv) 14__21

(*b*) Seja $S = (\mathbf{N}, \prec)$. Mostre que S é bem-ordenado.

(*c*) S possui elementos limite?

(*a*) Os elementos de $\mathbf{N}$ podem ser listados como na Fig. 14-14. A primeira linha consiste nos números ímpares, a segunda em 2 multiplicado por números ímpares, a terceira em $2^2 = 4$ vezes os números ímpares, e assim por diante. Então $a \prec a'$ se a está em uma linha superior, então a' ou se a e a' estão na mesma linha, mas a vem antes de a'. Portanto:

(i) $5 \prec 14$; (ii) $6 \succ 9$; (iii) $3 \succ 20$; (iv) $14 \succ 20$.

r \ s	0	1	2	3	4	5	6	7	
0	1	3	5	7	9	11	13	15	
1	2	6	10	14	18	22	26	30	
2	4	12	20	28	36	44	52	60	

Figura 14-14

(*b*) Seja A um subconjunto de S. As linhas são bem-ordenadas. Seja r_0 a denotação da linha mínima de elementos em A. Em r_0 podem existir vários elementos de A. As colunas são bem-ordenadas, então considere que s_0 denota a coluna mínima de elementos em A na linha r_0. Então $x = (r_0, s_0)$ é o primeiro elemento de A. Logo, S é bem-ordenado.

(*c*) Como indicado na Fig. 14-14, toda potência de 2, isto é, 1, 2, 4, 8,..., não possui predecessor imediato. Logo, cada número que não seja o 1 é um elemento limite de S.

14.21 Seja S um conjunto bem-ordenado. Considere que $f: S \to S$ é um mapeamento de similaridade de S em S. Prove que, para todo $a \in S$, temos $a \precsim f(a)$.

Seja $D = \{x \mid f(x) \prec x\}$. Se D é vazio, então a afirmação é verdadeira. Suponha que $D \neq \emptyset$. Uma vez que D é bem-ordenado, ele possui um primeiro elemento, digamos d_0. Uma vez que $d_0 \in D$, temos $f(d_0) \prec d_0$. Já que f é um mapeamento de similaridade:

$$f(d_0) \prec d_0 \text{ implica } f(f(d_0)) \prec f(d_0)$$

Logo, $f(d_0)$ também pertence a D. Mas $f(d_0) \prec d_0$ e $f(d_0) \in D$ contradiz o fato de que d_0 é o primeiro elemento de D. Daí a pressuposição original de que $D \neq \emptyset$ leva a uma contradição. Portanto, D é vazio e a afirmação é verdadeira.

14.22 Seja A um conjunto bem-ordenado. Considere que $s(A)$ denota a coleção de todos os segmentos iniciais $s(a)$ dos elementos $a \in A$ ordenados por inclusão de conjuntos. Prove que A é isomorfo a $s(A)$, mostrando que o mapa $f: A \to s(A)$, definido por $f(a) = s(a)$, é um mapeamento de similaridade de A em $s(A)$. (Compare com o Problema 14.17.)

Primeiro mostramos que f é um para um e sobrejetora. Suponha que $y \in s(A)$. Então $y = s(a)$ para algum $a \in A$. Logo, $f(a) = s(a) = y$, então f é sobrejetora em $s(A)$. Suponha que $x \neq y$. Então um precede o outro, digamos, $x \prec y$. Logo, $x \in s(y)$. Mas $x \notin s(x)$. Então $s(x) \neq s(y)$. Portanto, f é também um para um.

Agora precisamos apenas mostrar que f preserva a ordem, isto é,

$$x \precsim y \text{ se, e somente se, } s(x) \subseteq s(y)$$

Suponha que $x \precsim y$. Se $a \in s(x)$, então $a \prec x$ e, portanto $a \prec y$; logo, $a \in s(y)$. Então, $s(x) \subset s(y)$. Por outro lado, suponha que $x \not\precsim y$, isto é, $x \succ y$. Então $y \in s(x)$. Mas $y \notin s(y)$; portanto, $s(x) \not\subseteq s(y)$. Em outras palavras, $x \precsim y$ se, e somente se, $s(x) \subseteq s(y)$. Logo, f é um mapeamento de similaridade de A em $S(A)$ e, portanto, $A \cong s(A)$.

Reticulados

14.23 Escreva a dual de cada afirmação:

(a) $(a \wedge b) \vee c = (b \vee c) \wedge (c \vee a)$; ($b$) $(a \wedge b) \vee a = a \wedge (b \vee a)$.

Substitua $\vee$ por $\wedge$ e $\wedge$ por $\vee$ em cada afirmação para obter a declaração dual.

(a) $(a \vee b) \wedge c = (b \wedge c) \vee (c \wedge a)$; ($b$) $(a \vee b) \wedge a = a \vee (b \wedge a)$

14.24 Demonstre o Teorema 14.4: Seja L um reticulado. Então:

(i) $a \wedge b = a$ se, e somente se, $a \vee b = b$.

(ii) A relação $a \precsim b$ (definida por $a \wedge b = a$ ou $a \vee b = b$) é uma ordem parcial em L.

(i) Suponha que $a \wedge b = a$. Usando a Lei da Absorção no primeiro passo, temos:

$$b = b \vee (b \wedge a) = b \vee (a \wedge b) = b \vee a = a \vee b$$

Agora suponha que $a \vee b = b$. Novamente, usando a Lei da Absorção no primeiro passo, temos:

$$a = a \wedge (a \vee b) = a \wedge b$$

Logo, $a \wedge b = a$ se, e somente se, $a \vee b = b$.

(ii) Para qualquer a em L, temos $a \wedge a = a$ por idempotência. Logo, $a \precsim a$ e, portanto, $\precsim$ é reflexiva.

Suponha que $a \precsim b$ e $b \precsim a$. Então $a \wedge b = a$ e $b \wedge a = b$. Portanto, $a = a \wedge b = b \wedge a = b$ e, então, $\precsim$ é antissimétrica.

Em último lugar, suponha que $a \precsim b$ e $b \precsim c$. Então $a \wedge b = a$ e $b \wedge c = b$. Logo,

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$$

Portanto, $a \precsim c$ e, então $\precsim$ é transitiva. Consequentemente, $\precsim$ é uma ordem parcial em L.

14.25 Quais dos conjuntos parcialmente ordenados na Fig. 14-15 são reticulados?

Um conjunto parcialmente ordenado é um reticulado se, e somente se, sup (x, y) e inf (x, y) existem para cada par x, y no conjunto. Apenas (c) não é um reticulado, uma vez que $\{a, b\}$ possui três limites superiores, c, d e I, e nenhum deles precede os outros dois, isto é, sup (a, b) não existe.

14.26 Considere o reticulado L na Fig. 14-15(a).

(a) Quais elementos diferentes de zero são uniões irredutíveis?

(b) Quais elementos são átomos?

(a)

(b)

(c)

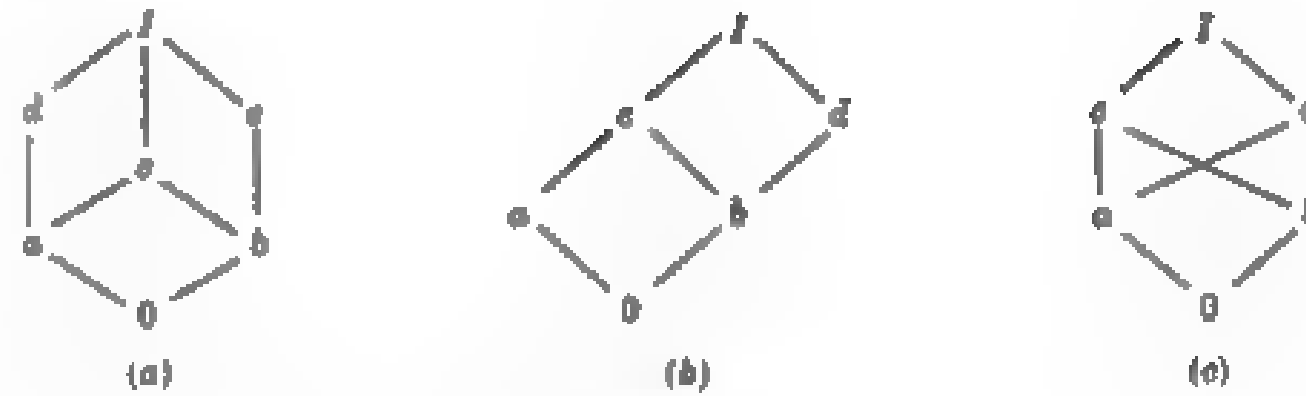



Figura 14-15

(c) Quais dos seguintes são subreticulados de L:

$$L_1 = \{0, a, b, I\}, \quad L_2 = \{0, a, e, I\}, \quad L_3 = \{a, c, d, I\}, \quad L_4 = \{0, c, d, I\}$$

(d) L é distributivo?

(e) Encontre complementares, se existirem, para os elementos a, b e c.

(f) L é um reticulado complementado?

(a) Os elementos diferentes de zero com um predecessor imediato único são uniões irredutíveis. Logo, a, b, d e e são uniões irredutíveis.

(b) Os elementos que sucedem imediatamente o 0 são átomos, logo, a e b são átomos.

(c) Um subconjunto L' é um subreticulado se for fechado sob $\wedge$ e $\vee$. L_1 não é um subreticulado, uma vez que $a \vee b = c$, que não pertence a L_1. O conjunto L_4 não é um subreticulado, uma vez que $c \wedge d = a$ não pertence a L_4. Os outros dois conjuntos, L_2 e L_3, são subreticulados.

(d) L não é distributivo, uma vez que $M = \{0, a, d, e, I\}$ é um subreticulado isomorfo ao reticulado não distributivo na Fig. 14-7(a).

(e) Temos $a \wedge e = 0$ e $a \vee e = I$, então a e e são complementares. De forma similar, b e d são complementares. Contudo, c não possui complementar.

(f) L não é um reticulado complementado, uma vez que c não possui complementar.

14.27 Considere o reticulado M na Fig. 14-15(b).

(a) Encontre os elementos diferentes de zero irredutíveis por união e átomos de M.

(b) M é (i) distributivo? (ii) complementado?

(a) Os elementos diferentes de zero com um único predecessor são a, b e d e, dos três, apenas a e b são átomos, uma vez que seu único predecessor é o 0.

(b) (i) M é distributivo, uma vez que M não possui subreticulados isomorfos a um dos reticulados na Fig. 14-7. (ii) M não é complementado, uma vez que b não possui complementar. Note que a é a única solução para $b \wedge x = 0$, mas $b \wedge a = c \neq I$.

14.28 Demonstre o Teorema 14.8: Seja L um reticulado finito distributivo. Então todo $a \in L$ pode ser escrito unicamente (exceto pela ordem) como a união de uniões não reduntantes irredutíveis.

Uma vez que L é finito, podemos escrever a como a união de uniões não redundantes irredutíveis, como discutido na Seção 14.9. Logo, precisamos provar sua unicidade. Suponha que

$$a = b_1 \vee b_2 \vee \cdots \vee b_r = c_1 \vee c_2 \vee \cdots \vee c_s$$

onde os b's são não redundantes e irredutíveis por união e os c's são não redundantes e irredutíveis. Para qualquer i, temos

$$b_i \preceq (b_1 \vee b_2 \vee \cdots \vee b_r) = (c_1 \vee c_2 \vee \cdots \vee c_s)$$

Logo,

$$b_i = b_i \wedge (c_1 \vee c_2 \vee \cdots \vee c_s) = (b_i \wedge c_1) \vee (b_i \wedge c_2) \vee \cdots \vee (b_i \wedge c_s)$$

Uma vez que b_i é irredutível por união, existe um j tal que $b_i = b_i \wedge c_j$ e, então, $b_i \precsim c_j$. Com um argumento similar, para c_j, existe um b_k tal que $c_j \precsim b_k$. Portanto,

$$b_i \precsim c_j \precsim b_k$$

que nos dá $b_i = c_{j_i} = b_k$, uma vez que os b's são não redundantes. Logo, os b's e os c's podem ser pareados. Portanto, a representação para a é única, exceto pela ordem.

14.29 Demonstre o Teorema 14.10: Seja L um reticulado complementado com complementares únicos. Então os elementos irredutíveis por união de L, que não sejam 0, são seus átomos.

Suponha que a é irredutível por união e a não é um átomo. Então a possui um único predecessor imediato $b \neq 0$. Seja b' o complemento de b. Uma vez que $b \neq 0$, temos $b' \neq I$. Se a precede b', então $b \precsim a \precsim b'$ e, portanto, $b \wedge b' = b$, que é impossível, uma vez que $b \wedge b' = I$. Logo, a não precede b' e, portanto, $a \wedge b'$ deve preceder imediatamente a. Uma vez que b é o único predecessor imediato de a, temos também que $a \wedge b'$ precede b, como na Fig. 14-16(a). Mas $a \wedge b'$ precede b'. Logo,

$$a \wedge b' \precsim \inf(b, b') = b \wedge b' = 0$$

Então $a \wedge b' = 0$. Uma vez que $a \vee b = a$, temos também que

$$a \vee b' = (a \vee b) \vee b' = a \vee (b \vee b') = a \vee I = I$$

Portanto, b' é um complemento de a. Uma vez que complementos são únicos, $a = b$. Isso contradiz a pressuposição de que b é um predecessor imediato de a. Logo, os únicos elementos irredutíveis por união de L são seus átomos.

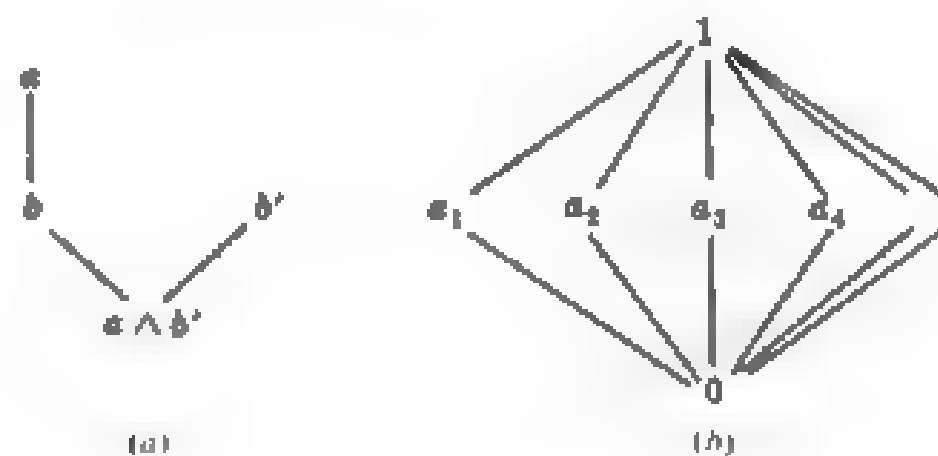



Figura 14-16

14.30 Dê exemplo de um reticulado L infinito, com comprimento finito.

Seja $L = \{0, 1, a_1, a_2, a_3, \ldots\}$, e considere que L é ordenado como na Fig. 14-16(b). Logo, para cada $n \in \mathbf{N}$, temos $0 < a_n < 1$. Então L possui um comprimento finito, uma vez que L não possui nenhum subconjunto infinito linearmente ordenado.

Problemas Complementares

Conjuntos ordenados e subconjuntos

14.31 Seja $A = \{1, 2, 3, 4, 5, 6\}$ ordenado como na Fig. 14-17(a).

(a) Encontre os elementos mínimos e máximos de A.

(b) A possui primeiro ou último elemento?

(c) Encontre todos os subconjuntos linearmente ordenados de A, cada um deles contendo, no mínimo, três elementos.

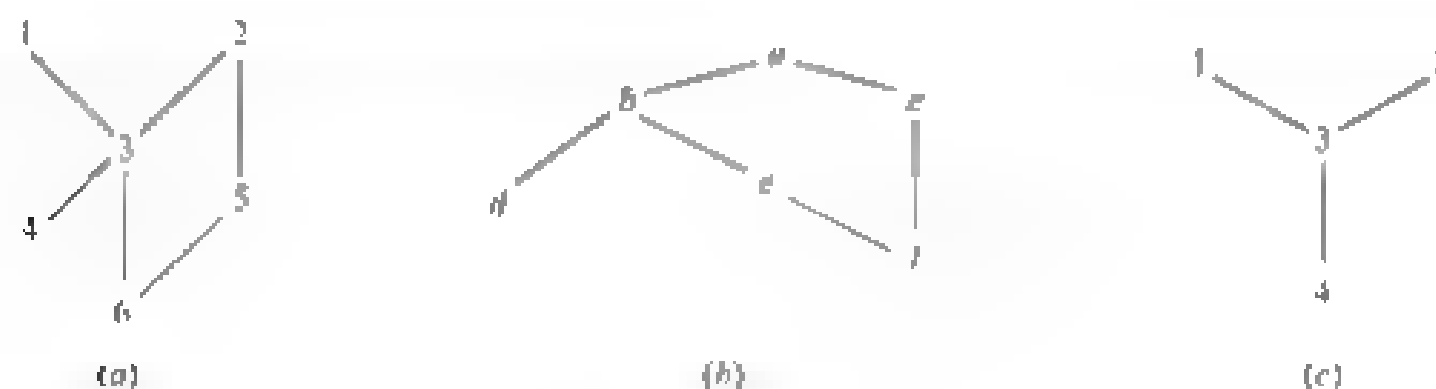



Figura 14-17

14.32 Seja $B = \{a, b, c, d, e, f\}$ ordenado como na Fig. 14-17(b).

(a) Encontre os elementos mínimos e máximos de B.

(b) B possui primeiro ou último elemento?

(c) Liste duas, mas encontre o número total de enumerações consistentes de B no conjunto $\{1, 2, 3, 4, 5, 6\}$

14.33 Seja $C = \{1, 2, 3, 4\}$ ordenado como na Fig. 14-17(c). Seja $L(C)$ a notação da coleção de todos os subconjuntos linearmente ordenados não vazios de C ordenados por inclusão de conjuntos. Esboce um diagrama de $L(C)$.

14.34 Esboce os diagramas das partições de m (veja o Exemplo 14.4) onde (a) $m = 4$, (b) $m = 6$.

14.35 Seja $\mathbf{D}_m$ a notação dos divisores positivos de m ordenados por divisibilidade. Esboce os diagramas de Hasse de:

(a) $\mathbf{D}_{12}$, (b) $\mathbf{D}_{15}$; (c) $\mathbf{D}_{16}$; (d) $\mathbf{D}_{17}$.

14.36 Seja $S = \{a, b, c, d, e, f\}$ um conjunto parcialmente ordenado. Suponha que existam exatamente seis pares de elementos onde o primeiro precede imediatamente o segundo, como se segue.

$$f \ll a, \quad f \ll d, \quad e \ll b, \quad c \ll f, \quad e \ll c, \quad b \ll f$$

(a) Encontre os elementos mínimos e máximos de S.

(b) S possui primeiro ou último elemento?

(c) Encontre todos os pares de elementos, se existirem, que são não comparáveis.

14.37 Determine se as afirmações a seguir são verdadeiras ou falsas e, no caso de serem falsas, dê um contraexemplo.

(a) Se um conjunto parcialmente ordenado S possui apenas um elemento máximo a, então a é seu último elemento.

(b) Se um conjunto parcialmente ordenado finito S possui apenas um elemento máximo a, então a é seu último elemento.

(c) Se um conjunto S linearmente ordenado possui apenas um elemento máximo a, então a é seu último elemento

14.38 Seja $S = \{a, b, c, d, e\}$ ordenado como na Fig. 14-18(a).

(a) Encontre todos os elementos mínimos e máximos de S.

(b) S possui primeiro ou último elemento?

(c) Encontre todos os subconjuntos de S em que c é um elemento mínimo.

(d) Encontre todos os subconjuntos de S em que c é um primeiro elemento.

(e) Liste todos os subconjuntos linearmente ordenados com três ou mais elementos.

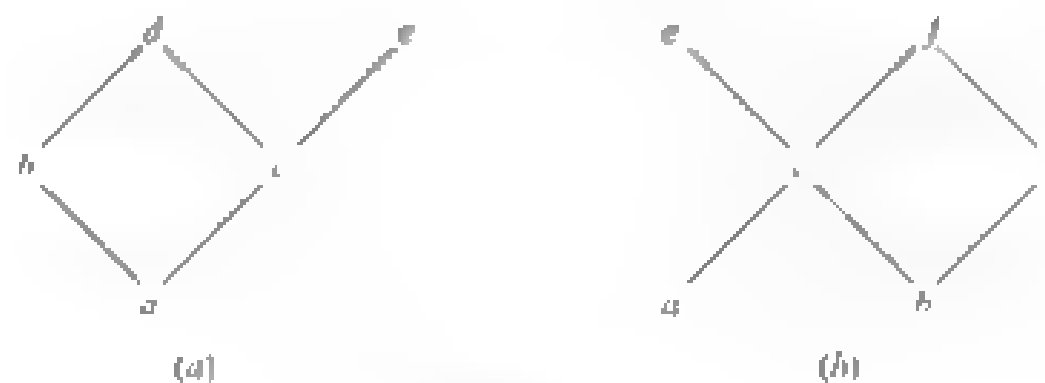



Figura 14-18

14.39 Seja $S = \{a, b, c, d, e, f\}$ ordenado como na Fig. 14-18(b).

(a) Encontre todos os elementos mínimos e máximos de S

(b) S possui primeiro ou último elemento?

(c) Liste todos os subconjuntos linearmente ordenados com três ou mais elementos.

14.40 Seja $S = \{a, b, c, d, e, f, g\}$ ordenado como na Fig. 14-11(a). Encontre o número n de subconjuntos linearmente ordenados de S com:

(a) quatro elementos, (b) cinco elementos.

14.41 Seja $S = \{1, 2, \ldots, 7, 8\}$ ordenados como na Fig. 14-11(b). Encontre o número n de subconjuntos linearmente ordenados de S com:

(a) cinco elementos; (b) seis elementos.

Enumerações consistentes

14.42 Seja $S = \{a, b, c, d, e\}$ ordenado como na Fig. 14-18(a). Liste todas as enumerações consistentes de S em $\{1, 2, 3, 4, 5\}$.

14.43 Seja $S = \{a, b, c, d, e, f\}$ ordenado como na Fig. 14-18(b). Encontre o número n de enumerações consistentes de S em $\{1, 2, 3, 4, 5, 6\}$.

14.44 Suponha que a seguir temos três enumerações consistentes de um conjunto ordenado $A = \{a, b, c, d\}$:

$$[(a, 1), (b, 2), (c, 3), (d, 4)], \quad [(a, 1), (b, 3), (c, 2), (d, 4)], \quad [(a, 1), (b, 4), (c, 2), (d, 3)]$$

Assumindo que o diagrama de Hasse D de A é conexo, esboce D.

Ordem e conjuntos produto

14.45 Seja $M = \{2, 3, 4, \ldots\}$ e considere que $M^2 = M \times M$ é ordenado como se segue:

$$(a, b) \prec (c, d) \quad \text{se } a \mid c \text{ e } b \leq d$$

Encontre todos os elementos mínimos e máximos de $M \times M$.

14.46 Considere o alfabeto $A = \{a, b, c, \ldots, y, z\}$ com a ordem usual (alfabética). Lembre-se de que A^* consiste em todas as palavras em A. Considere que L consiste na seguinte lista de elementos em A^*:

gone, or, arm, go, an, about, gate, one, at, occur

(a) Organize L de acordo com a ordem léxica, ou seja, por comprimento e, em seguida, alfabeticamente.

(b) Organize L alfabeticamente.

14.47 Considere os conjuntos ordenados A e B que aparecem na Fig. 14-17(a) e (b), respectivamente. Suponha que $S = A \times B$ é dado pela ordem de produto. Insira o símbolo correto, $\prec$, $\succ$ ou $\|$, entre cada par de elementos de S:

(a) $(4, b)$___$(2, e)$; (b) $(3, a)$___$(6, f)$; (c) $(5, d)$___$(1, a)$; (d) $(6, e)$___$(2, b)$.

14.48 Suponha que $\mathbf{N} = \{1, 2, 3, \ldots\}$ e $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ são organizados pelas suas ordens usuais, e $S = \mathbf{N} \times \mathbf{A}$ é ordenado lexicograficamente. Organize os seguintes elementos de S:

$$(2, z), \quad (1, c), \quad (2, c), \quad (1, y), \quad (4, b), \quad (4, z), \quad (3, b), \quad (2, a)$$

Limites superiores e inferiores, supremo e ínfimo

14.49 Seja $S = \{a, b, c, d, e, f, g\}$ ordenado como na Fig. 14-11(a). Considere que $A = \{a, c, d\}$.

(a) Encontre o conjunto de limites superiores de A.

(b) Encontre o conjunto de limites inferiores de A.

(c) sup (A) existe?

(d) inf (A) existe?

14.50 Repita o Problema 14.49 para o subconjunto $B = \{b, c, e\}$ de S.

14.51 Seja $S = \{1, 2, \ldots, 7, 8\}$ ordenado como na Fig. 14-11(b). Considere o subconjunto $A = \{3, 6, 7\}$ de S.

(a) Encontre o conjunto de limites superiores de A.

(b) Encontre o conjunto de limites inferiores de A.

(c) sup (A) existe?

(d) inf (A) existe?

14.52 Repita o Problema 14.51 para o subconjunto $B = \{1, 2, 4, 7\}$ de S.

14.53 Considere os números racionais **Q** com a ordem usual $\leq$. Seja $A = \{x \mid x \in \mathbf{Q} \text{ e } 5 < x^3 < 27\}$

(a) A possui limite superior ou inferior?

(b) sup (A) ou inf (A) existem?

14.54 Considere os números reais **R** com a ordem usual $\leq$. Seja $A = \{x \mid x \in \mathbf{Q} \text{ e } 5 < x^3 < 27\}$

(a) A é delimitado acima ou abaixo? (b) sup (A) ou inf (A) existem?

Conjuntos isomorfos (similares), mapeamento de similaridades

14.55 Encontre o número de conjuntos parcialmente ordenados não isomorfos com três elementos a, b e c e esboce os respectivos diagramas.

14.56 Encontre o número de conjuntos parcialmente ordenados não isomorfos conexos com quatro elementos a, b, c e d e esboce os respectivos diagramas.

14.57 Encontre o número de mapeamentos de similaridades $f: S \to S$ onde S é o conjunto ordenado em

(a) Fig. 14-17(a); (b) Fig. 14-17(b); (c) Fig. 14-17(c)

14.58 Mostre que a relação isomorfa $A \cong B$ para conjuntos ordenados é uma relação de equivalência, isto é

(a) $A \cong A$ para qualquer conjunto ordenado A (b) Se $A \cong B$, então $B \cong A$. (c) Se $A \cong B$ e $B \cong C$, então $A \cong C$.

Conjuntos bem-ordenados

14.59 Seja a união S dos conjuntos $A = \{a_1, a_2, a_3, \ldots\}$, $B = \{b_1, b_2, b_3, \ldots\}$ e $C = \{c_1, c_2, c_3, \ldots\}$ ordenada por

$$S = \{A; B; C\} = \{a_1, a_2, \ldots, b_1, b_2, \ldots, c_1, c_2, \ldots\}$$

(a) Mostre que S é bem-ordenado.

(b) Encontre todos os elementos limite de S.

(c) Mostre que S não é isomorfo a $\mathbf{N} = \{1, 2, \ldots\}$ com a ordem usual $\leq$.

14.60 Seja $A = \{a, b, c\}$ linearmente ordenado por $a < b < c$ e considere que **N** possui a ordem usual $\leq$.

(a) Mostre que $S = \{A; \mathbf{N}\}$ é isomorfo a **N**.

(b) Mostre que $S' = \{\mathbf{N}, A\}$ não é isomorfo a **N**.

14.61 Suponha que A é um conjunto bem-ordenado sob a relação $\precsim$ e que A é, também, bem-ordenado sob a relação inversa $\succsim$. Descreva A.

14.62 Suponha que A e B são conjuntos isomorfos bem-ordenados. Mostre que existe apenas um mapeamento de similaridade $f: A \to B$.

14.63 Seja S um conjunto bem-ordenado. Para qualquer $a \in S$, o conjunto $s(a) = \{x \mid x \prec a\}$ é chamado de *segmento inicial* de a. Mostre que S não pode ser isomorfo a um de seus *segmentos iniciais*. (*Sugestão*: Use o Problema 14.21.)

14.64 Suponha que $s(a)$ e $s(b)$ são segmentos iniciais distintos de um conjunto S bem-ordenado. Mostre que $s(a)$ e $s(b)$ não podem ser isomorfos. (*Sugestão*: Use o Problema 14.63.)

Reticulados

14.65 Considere o reticulado L na Fig. 14-19(a).

(a) Encontre todos os subreticulados com cinco elementos.

(b) Encontre todos os elementos irredutíveis por união e átomos.

(c) Encontre os complementos de a e b, caso existam.

(d) L é distributivo? e complementado?

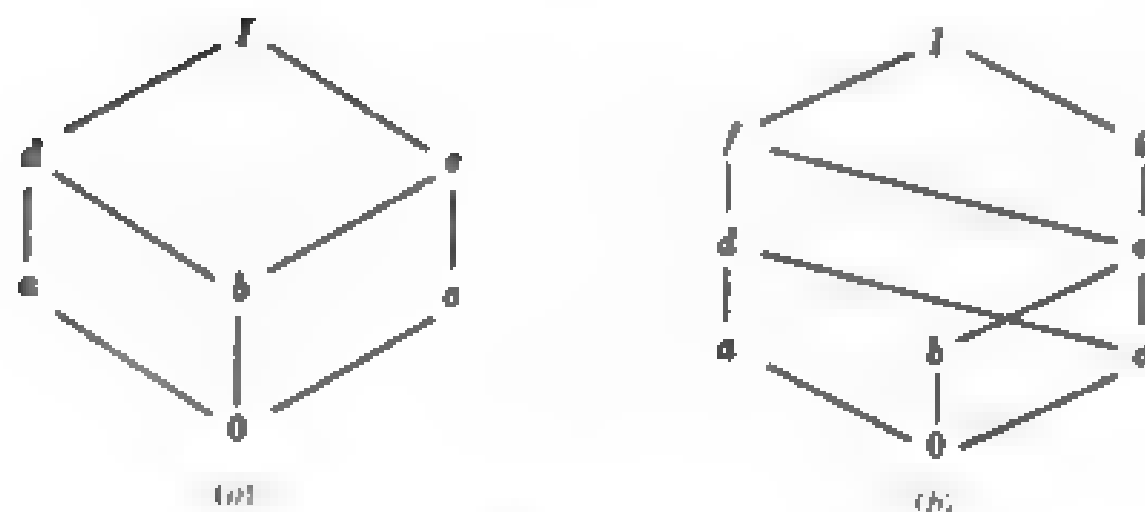



Figura 14-19

14.66 Considere o reticulado M na Fig. 14-19(b).

(a) Encontre todos os elementos irredutíveis por união.

(b) Encontre os átomos.

(c) Encontre os complementares de a e b, caso existam.

(d) Expresse cada x em M como a união de elementos não redundantes irredutíveis por união.

(e) M é distributivo? e complementado?

14.67 Considere o reticulado L no limite da Fig. 14-20(a).

(a) Encontre os complementares, caso existam, de e e f

(b) Expresse I em uma decomposição irredutível por união no maior número de maneiras possível.

(c) L é distributivo?

(d) Descreva os isomorfismos de L com ele mesmo.

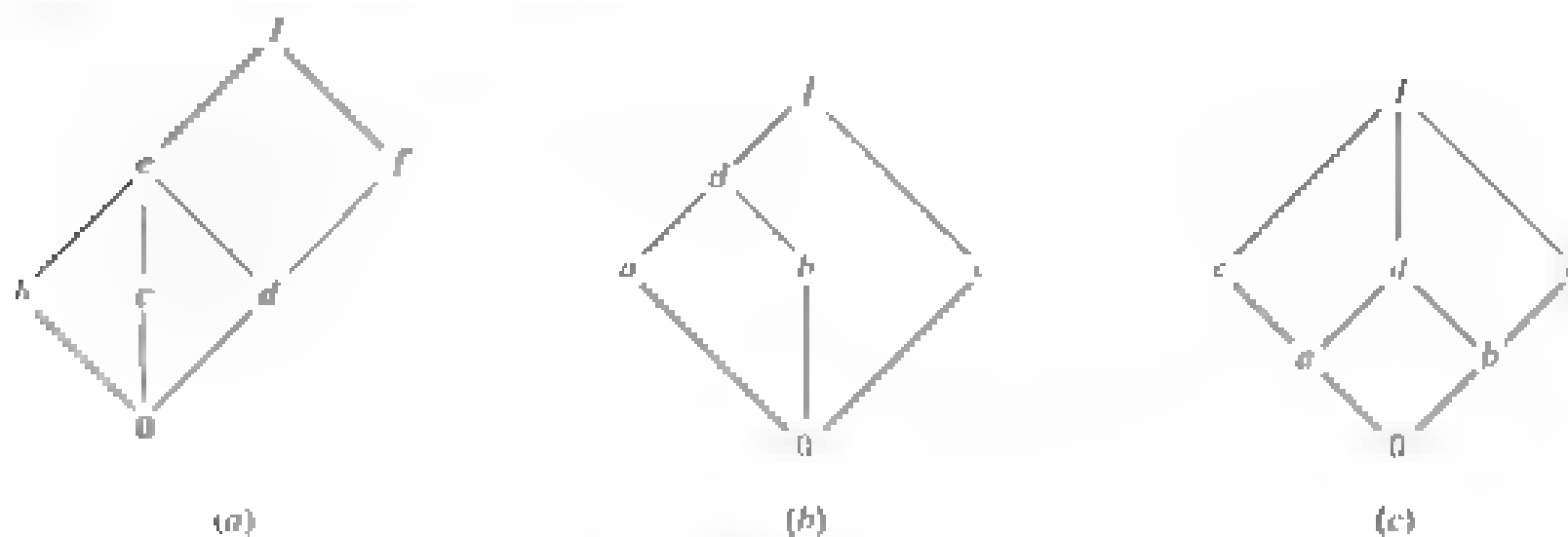



Figura 14-20

14.68 Considere o reticulado L no limite da Fig. 14-20(b).

(a) Encontre os complementares, caso existam, de a e c.

(b) Expresse I em uma decomposição não redundante e irredutível por união no maior número de maneiras possível

(c) L é distributivo?

(d) Descreva os isomorfismos de L com ele mesmo.

14.69 Considere o reticulado L no limite da Fig. 14-20(c).

(a) Encontre os complementares, caso existam, de a e c.

(b) Expresse I em uma decomposição não redundante e irredutível por união no maior número de maneiras possível.

(c) L é distributivo?

(d) Descreva os isomorfismos de L com ele mesmo.

14.70 Considere o reticulado $D_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$, os divisores de 60 ordenados por divisibilidade.

(a) Esboce o diagrama de D_{60}.

(b) Quais elementos são irredutíveis por união e quais são átomos?

(c) Encontre os complementos de 2 e de 10, caso existam.

(d) Expresse cada número x como a união de um número mínimo de elementos não redundantes irredutíveis por união.

14.71 Considere o reticulado **N** de inteiros positivos ordenados por divisibilidade.

(a) Quais elementos são irredutíveis por união?

(b) Quais elementos são átomos?

14.72 Mostre que as seguintes leis distributivas "fracas" são válidas para qualquer reticulado L.

(a) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$, (b) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$.

14.73 Seja $S = \{1, 2, 3, 4\}$. Usamos a notação $[12, 3, 4] \equiv [\{1, 2\}, \{3\}, \{4\}]$. Três partições de S são listadas a seguir:

$$P_1 = [12, 3, 4], \quad P_2 = [12, 34], \quad P_3 = [13, 2, 4]$$

(a) Encontre as outras doze partições de S.

(b) Seja L uma coleção das 12 partições de S ordenada por *refinamento*, isto é, $P_i \prec P_j$ se cada célula de P_i é um subconjunto de uma célula de P_j. Por exemplo, $P_1 \prec P_2$, mas P_2 e P_3 são não comparáveis. Mostre que L é um reticulado delimitado e esboce seu diagrama.

14.74 Um elemento a em um reticulado L é dito irredutível por interseção se $a = x \wedge y$ implica $a = x$ ou $a = y$. Encontre todos os elementos irredutíveis por intereseção em, (a) Fig. 14-19(a); (b) Fig. 14-19(b). (c) D_{60} (veja o Problema 14.70.)

14.75 Um reticulado M é dito *modular* se, quando $a \leq c$, temos a lei

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

(a) Prove que todo reticulado distributivo é modular.

(b) Comprove que o reticulado não distributivo na Fig. 14-7(b) é modular; logo, a recíproca de (a) não é verdadeira.

(c) Mostre que o reticulado não distributivo na Fig. 14-7(a) é não modular. (Na verdade, é possível provar que todo reticulado não modular contém um subreticulado isomorfo à Fig. 14-7(a).)

14.76 Seja R um anel. Considere que L é a coleção de todos os ideais de R. Prove que L é um reticulado cotado onde, para quaisquer ideais J e K de R, definimos: $J \vee K = J + K$ e $J \wedge K = J \cap K$.

Respostas dos Problemas Complementares

14.31 (a) Mínimo, 4 e 6; máximo, 1 e 2. (b) Primeiro, nenhum; último, nenhum. (c) $\{1, 3, 4\}$, $\{1, 3, 6\}$, $\{2, 3, 4\}$, $\{2, 3, 6\}$, $\{2, 5, 6\}$.

14.32 (a) Mínimo, d e f; máximo, a. (b) Primeiro, nenhum; último, a. (c) Existem onze: *dfebca*, *dfecba*, *dfceba*, *fdebca*, *fdecba*, *fdceba*, *fedbca*, *fedcba*, *fcdeba*, *fecdba* e *fcedba*.

14.33 Veja a Fig. 14-21.

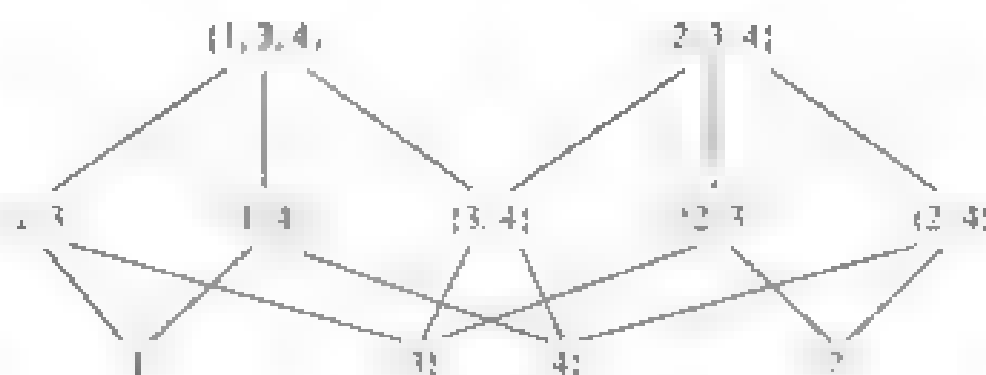



Figura 14-21

14.34 Veja a Fig. 14-22.

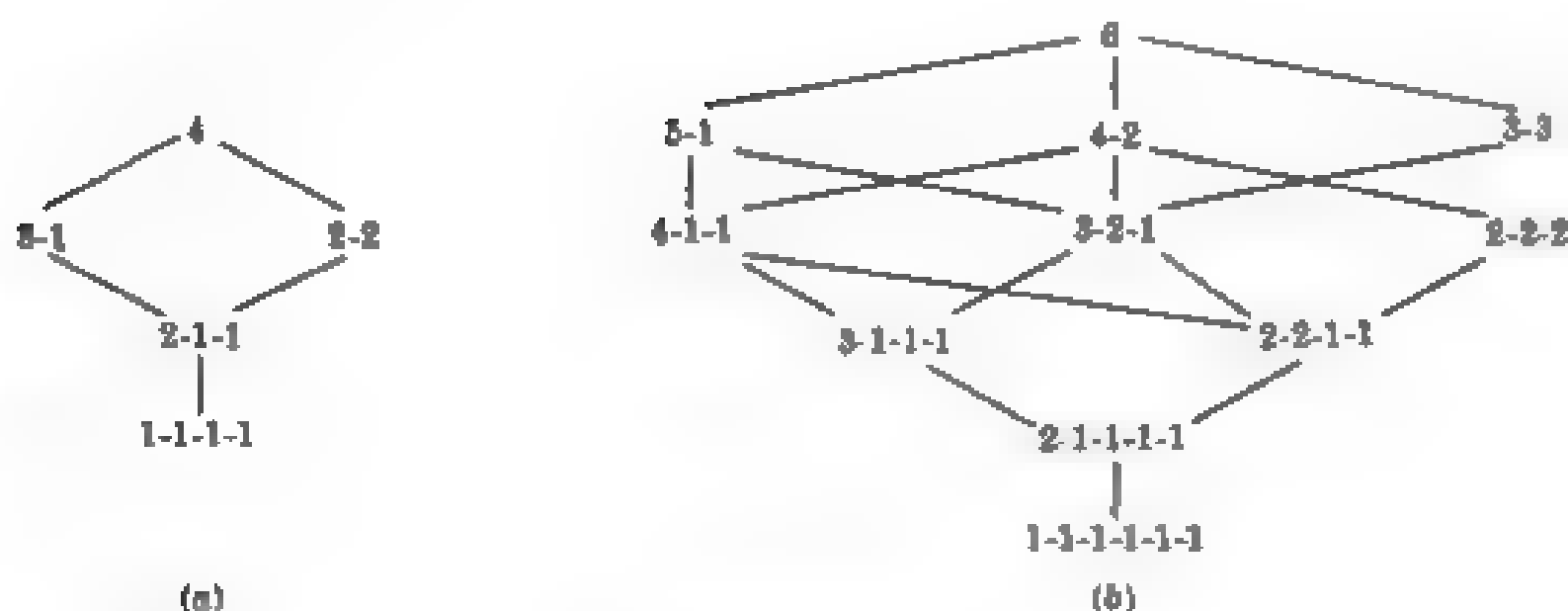



Figura 14-22

14.35 Veja a Fig. 14-23.

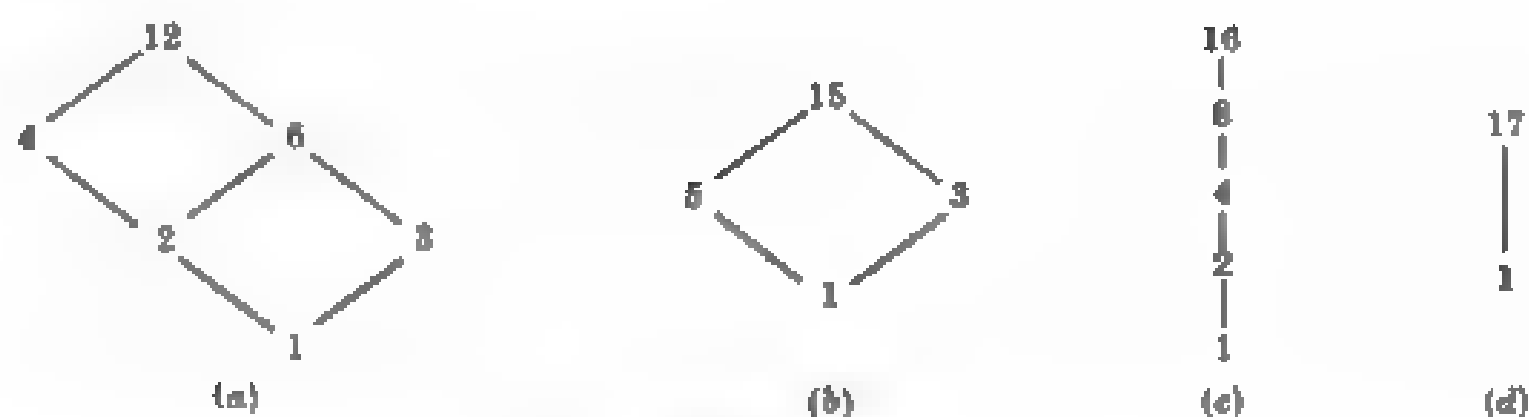



Figura 14-23

14.36 *Sugestão*: Esboce o diagrama de *S*.

(a) Mínimo, *e*; máximo, *a* e *d*.

(b) Primeiro, *e*; último, nenhum.

(c) $\{a, d\}$, $\{b, c\}$

14.37 (a) Falso. Exemplo. $\mathbf{N} \cup \{a\}$ onde $1 \ll a$ e $\mathbf{N}$ ordenado por $\leq$. (b) Verdadeiro. (c) Verdadeiro.

14.38 (a) Mínimo, *a*, máximo, *d* e *e*. (b) Primeiro, *a*; último, nenhum. (c) Qualquer subconjunto que contenha *c* e omita *a*, isto é: *c*, *cb*, *cd*, *ce*, *cbd*, *cde*, *cbde*. (d) *c*, *cd*, *ce*, *cde*. (e) *abd*, *acd*, *ace*.

14.39 (a) Mínimo, *a* e *b*; máximo, *e* e *f*. (b) Primeiro, nenhum, último, nenhum. (c) *ace*, *acf*, *bce*, *bcf*, *bdf*

14.40 (a) Quatro. (b) Nenhum.

14.41 (a) Seis. (b) Nenhum.

14.42 *abcde*, *abced*, *acbde*, *acbed* e *acebd*

14.43 Onze.

14.44 $a \ll b$, $a \ll c$, $c \ll d$.

14.45 Mínimo, $(p, 2)$ onde p é primo. Máximo, nenhum.

14.46 (a) an, at, go, or, arm, one, gate, gone, about, occur.
(b) an, about, arm, at, gate, go, gone, occur, one, or.

14.47 (a) $\|$; (b) $>$; (c) $|$; (d) $<$.

14.48 $1c$, $1y$, $2a$, $2c$ $2z$, $3b$, $4b$ e $4z$

14.49 (a) e, f e g; (b) a; (c) $\sup(A) = e$; (d) $\inf(A) = a$.

14.50 (a) e, f e g; (b) nenhum; (c) $\sup(B) = e$; (d) nenhum.

14.51 (a) 1, 2 e 3; (b) 8; (c) $\sup(A) = 3$. (d) $\inf(A) = 8$.

14.52 (a) Nenhum. (b) 8; (c) nenhum; (d) $\inf(B) = 8$.

14.53 (a) Ambos; (b) $\sup(A) = 3$; $\inf(A)$ não existe.

14.54 (a) Ambos; (b) $\sup(A) = 3$; $\inf(A) = \sqrt[3]{5}$

14.55 Quatro: (1) a, b e c; (2) $a, b \ll c$; (3) $a \ll b, a \ll c$. (4) $a \ll b \ll c$.

14.56 Quatro: Veja a Fig. 14-24.

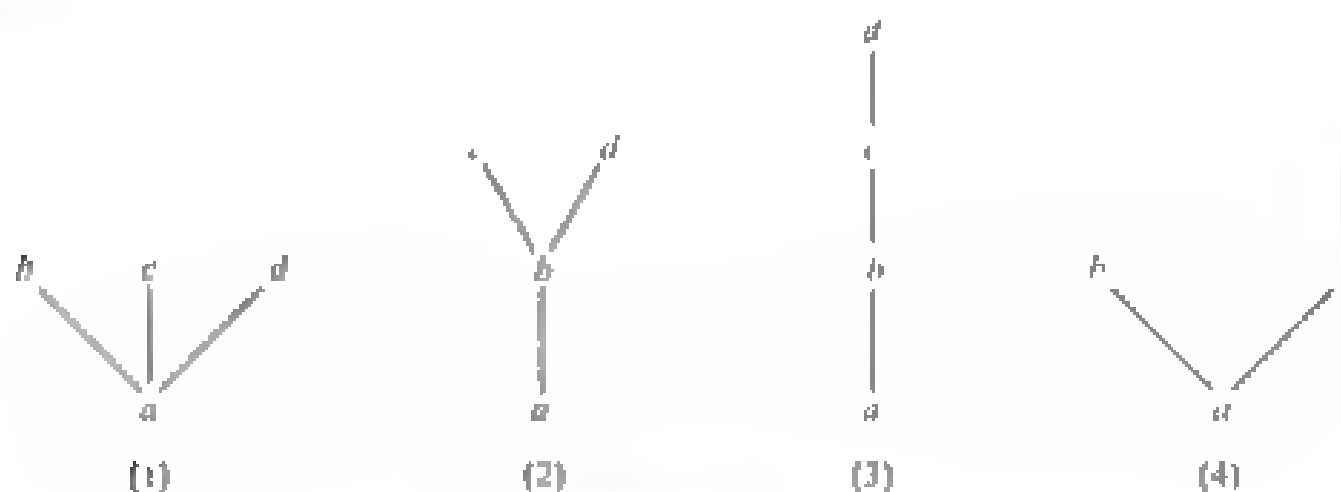



Figura 14-24

14.57 (a) Um: Mapeamento de identidade; (b) um; (c) dois.

14.59 (b) b_1, c_1, (c) **N** não possui pontos limite.

14.60 (a) Defina $f: S \to \mathbf{N}$ por $f(a) = 1$, $f(b) = 2$, $f(3) = 3$, $f(n) = n + 3$.
(b) O elemento a é um ponto limite de S', mas **N** não possui pontos limite.

14.61 A é um conjunto finito linearmente ordenado.

14.65 (a) Seis. $0abd1$, $0acd1$, $0ade1$, $0bce1$, $0ace1$, $0cde1$. (b) (i) $a, b, c, 0$; (ii) $a, b, c, 0$, (c) c e e são complementos de a. b não possui complementos. (d) Não. Não.

14.66 (a) $a, b, c, g, 0$. (b) a, b, c (c) a possui g; b não possui nenhum. (d) $I = a \vee g$, $f = a \vee b$, $e = b \vee c$, $d = a \vee c$ Outros elementos são irredutíveis por união. (e) Não. Não.

14.67 (a) e não possui nenhum, f possui b e c (b) $I = c \vee f = b \vee f = b \vee d \vee f$ (c) Não, uma vez que decomposições não são únicas. (d) Dois: $0, d, e, f, I$ devem ser mapeados neles mesmos. Então $F = 1_L$, idenfique o mapa em L ou $F = \{(b, c), (c, b)\}$

14.68 (a) a possui c, c possui a e b. (b) $I = a \vee c = b \vee c$ (c) Não. (d) Dois: $0, c, d, I$ devem ser mapeados neles mesmos. Então $f = 1_L$ ou $f = \{(a, b), (b, a)\}$.

14.69 (a) a possui e, c possui b e e. (b) $I = a \vee e = b \vee c = c \vee e$. (c) Não. (d) Dois. $0, d, I$ são mapeados neles mesmos. Então $f = 1_L$ ou $f = \{(a, b), (b, a), (c, d), (d, c)\}$.

14.70 (a) Veja a Fig. 14-25. (b) 1, 2, 3, 4, 5. Os átomos são 2, 3 e 5. (c) 2 não possui nenhum, 10 também não possui nenhum. (d) $60 = 4 \vee 3 \vee 5$, $30 = 2 \vee 3 \vee 5$, $20 = 4 \vee 5$; $15 = 3 \vee 5$; $12 = 3 \vee 4$; $10 = 2 \vee 5$; $6 = 2 \vee 3$.

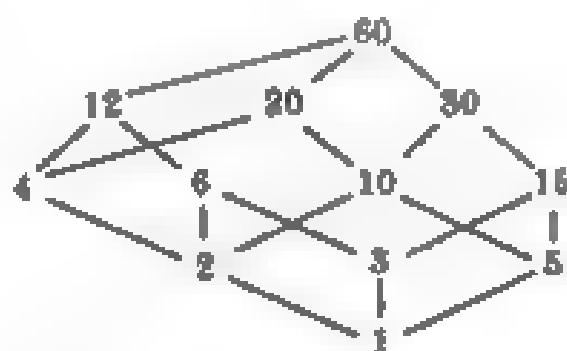



Figura 14-25

14.73 (a) [1, 2, 3, 4], [14, 2, 3], [13, 24], [14, 23], [123, 4], [124, 3], [134, 2], [234, 1], [1234], [23, 1, 4] [24, 1, 3], [34, 1, 2] (b) Veja a Fig. 14-26.

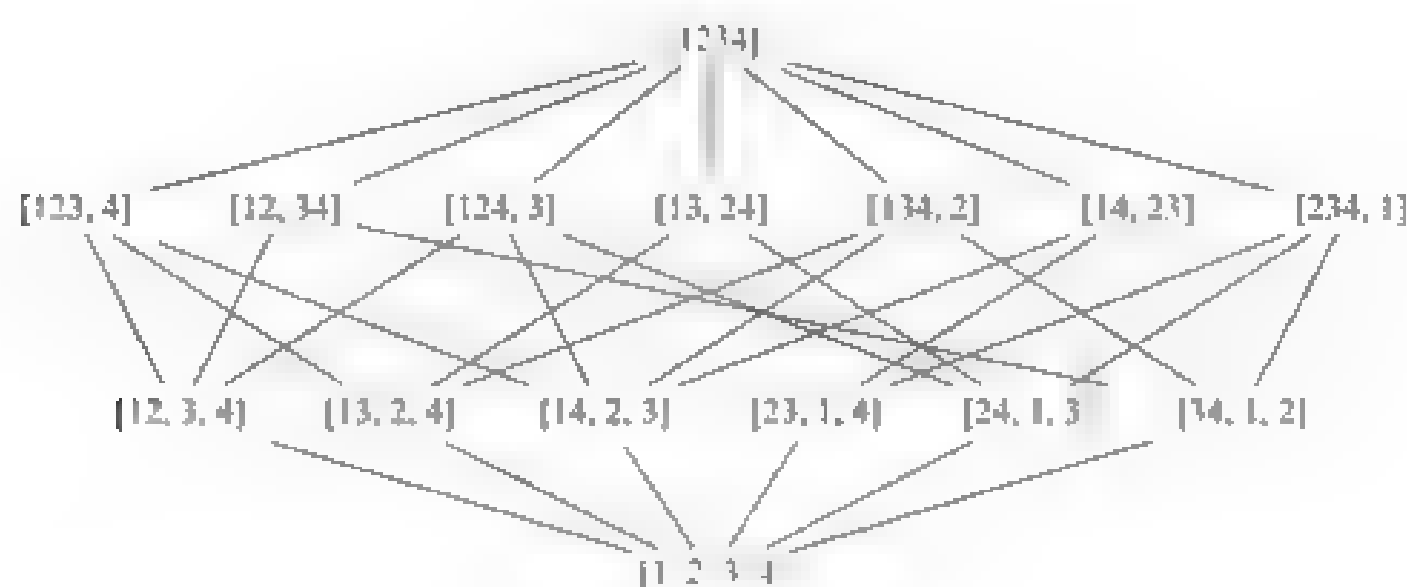



Figura 14-26

14.74 Geometricamente, um elemento $a \neq I$ é irredutível por interseção se, e somente se, a possui apenas um sucessor imediato. (a) a, c, d, e, I; (b) a, b, d, f, g, I; (c) 4, 6, 12, 15, 60.

14.75 (a) Se $a < c$, então $a \vee c = c$. Logo, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$; (b) Aqui $a < c$. Mas $a \vee (b \wedge c) = a \vee 0 = a$ e $(a \vee b) \wedge c = I \wedge c = c$; logo, $a \vee (b \wedge c) \neq (a \vee b) \wedge c$

Álgebra Booleana

15.1 INTRODUÇÃO

Tanto conjuntos quanto proposições satisfazem leis similares, que são listadas nas Tabelas 1-1 e 4-1 (nos Capítulos 1 e 4, respectivamente). Essas leis são usadas para definir uma estrutura matemática abstrata chamada de *álgebra Booleana*, batizada em homenagem ao matemático George Boole (1815-1864).

15.2 DEFINIÇÕES BÁSICAS

Seja B um conjunto não vazio com duas operações binárias, $+$ e $*$, uma operação unária $'$ e dois elementos distintos, 0 e 1. Então B é chamado de *álgebra Booleana* se os axiomas a seguir forem válidos, onde a, b e c são quaisquer elementos em B:

[B_1] Leis Comutativas:
(1a) $a + b = b + a$ (1b) $a * b = b * a$

[B_2] Leis Distributivas:
(2a) $a + (b * c) = (a + b) * (a + c)$ (2b) $a * (b + c) = (a * b) + (a * c)$

[B_3] Leis de Identidade:
(3a) $a + 0 = a$ (3b) $a * 1 = a$

[B_4] Leis de Complemento:
(4a) $a + a' = 1$ (4b) $a * a' = 0$

Às vezes, designamos uma álgebra Booleana com $\langle B, +, *, ', 0, 1\rangle$, quando queremos enfatizar suas seis partes. Dizemos que 0 é o elemento *zero*, 1 é o elemento *unitário* e a' é o *complementar* de a. Normalmente descartamos o símbolo $*$ e, em vez dele, usamos justaposição. Então (2b) é escrito na forma $a(b + c) = ab + ac$, que é a identidade algébrica já conhecida de anéis e corpos. Contudo, (2a) torna-se $a + bc = (a + b)(a + c)$, que certamente não é uma identidade usual em álgebra.

As operações $+$, $*$ e $'$ são chamadas de soma, produto e complementar, respectivamente. Adotamos a convenção de que, a menos que sejamos guiados por parênteses, $'$ possui precedência sobre $*$ e $*$ possui precedência sobre $+$. Por exemplo,

$$a + b * c \text{ significa } a + (b * c), \text{ e não } (a + b) * c; \quad a * b' \text{ significa } a * (b'), \text{ e não } a * (b)'$$

Certamente, quando $a + b * c$ é escrita na forma $a + bc$, seu significado fica claro.

Exemplo 15.1

(a) Seja $\mathbf{B} = \{0, 1\}$, o conjunto de *bits* (dígitos binários), com as operações binárias $+$ e $*$ e a operação unária $'$ definida pela Fig. 15-1. Então $\mathbf{B}$ é uma álgebra Booleana. (Note que $'$ apenas muda o bit, ou seja, $1' = 0$ e $0' = 1$.)

+	1	0
1	1	1
0	1	0

*	1	0
1	1	0
0	0	0

'	1	0
	0	1

Figura 15-1

(b) Seja $\mathbf{B}^n = \mathbf{B} \times \mathbf{B} \times \cdots \times \mathbf{B}$ (n fatores) onde as operações de $+$, $*$ e $'$ são definidas de acordo com as componentes, usando a Fig. 15-1. Por conveniência de notação, escrevemos os elementos de $\mathbf{B}^n$ como sequências de n bits sem vírgulas, por exemplo, $x = 110011$ e $y = 111000$ pertencem a $\mathbf{B}^n$. Logo,

$$x + y = 111011, \quad x * y = 110000, \quad x' = 001100$$

Então $\mathbf{B}^n$ é uma álgebra Booleana. Aqui $0 = 000 \cdots 0$ é o elemento zero e $1 = 111 \cdots 1$ é o elemento unitário. Notamos que $\mathbf{B}^n$ possui 2^n elementos.

(c) Seja $\mathbf{D}_{70} = \{1, 2, 5, 7, 10, 14, 35, 70\}$, os divisores de 70. Defina $+$, $*$ e $'$ em $\mathbf{D}_{70}$ por

$$a + b = \text{mmc}(a, b), \quad a * b = \text{mdc}(a, b), \quad a' = \frac{70}{a}$$

Então $\mathbf{D}_{70}$ é uma álgebra Booleana com 1 como o elemento zero e 70 como o elemento unitário.

(d) Seja C uma coleção de conjuntos fechada sob as operações de união, interseção e complementar. Então C é uma álgebra Booleana com o conjunto vazio $\varnothing$ como o elemento zero e o conjunto universo U como o elemento unitário.

Subálgebras, álgebras Booleanas isomorfas

Suponha que C é um subconjunto não vazio de uma álgebra Booleana B. Dizemos que C é uma *subálgebra* de B se C é, também, uma álgebra Booleana (em relação às operações de B). Notamos que C é uma subálgebra de B se, e somente se, C é fechado sob as três operações de B, isto é, $+$, $*$ e $'$. Por exemplo, $\{1, 2, 35, 70\}$ é uma subálgebra de $\mathbf{D}_{70}$ no Exemplo 15.1(c).

Duas álgebras Booleanas B e B' são ditas *isomorfas* se existe uma correspondência de um para um $f: B \to B'$ que preserva as três operações, ou seja, tal que, para quaisquer elementos a e b em B,

$$f(a + b) = f(a) + f(b), \quad f(a * b) = f(a) * f(b) \quad \text{e} \quad f(a') = f(a)'$$

15.3 DUALIDADE

A *dual* de qualquer declaração em uma álgebra Booleana B é a declaração obtida pela permutação das operações $+$ e $*$, e permutando seus elementos identidade 0 e 1 na declaração original. Por exemplo, a dual de

$$(1 + a) * (b + 0) = b \text{ é } (0 * a) + (b * 1) = b$$

Observe a simetria nos axiomas de uma álgebra Booleana B. Isto é, a dual de um conjunto de axiomas de B é o mesmo que o conjunto original de axiomas. Logo, o importante Princípio de Dualidade é válido em B.

Teorema 15.1 (Princípio de Dualidade): A dual de qualquer teorema em uma álgebra Booleana é também um teorema.

Em outras palavras, se qualquer declaração é consequência dos axiomas de uma álgebra Booleana, então a dual também é uma consequência desses axiomas, uma vez que a declaração dual pode ser provada, usando a dual de cada passo da demonstração da declaração original.

15.4 TEOREMAS BÁSICOS

Usando os axiomas $[\mathbf{B_1}]$ até o $[\mathbf{B_4}]$, provamos (Problema 15.5) o seguinte teorema.

Teorema 15.2: Sejam a, b e c quaisquer elementos em uma álgebra Booleana B.

(i) Leis da Idempotência

$(5a)\ a + a = a$ $\qquad$ $(5b)\ a * a = a$

(ii) Leis de Limites:

$(6a)\ a + 1 = 1$ $\qquad$ $(6b)\ a * 0 = 0$

(iii) Leis de Absorção:

$(7a)\ a + (a * b) = a$ $\qquad$ $(7b)\ a * (a + b) = a$

(iv) Leis Associativas.

$(8a)\ (a + b) + c = a + (b + c)$ $\qquad$ $(8b)\ (a * b) * c = a * (b * c)$

O Teorema 15.2 e os nossos axiomas não contêm todas as propriedades de conjuntos listadas na Tabela 1-1. Os próximos dois teoremas nos dão as propriedades restantes.

Teorema 15.3: Seja a qualquer elemento em uma álgebra Booleana B

(i) (Unicidade de Complemento) Se $a + x = 1$ e $a * x = 0$, então $x = a'$.

(ii) (Lei de Involução) $(a')' = a$.

(iii) $(9a)\ 0' = 1$, $(9b)\ 1' = 0$.

Teorema 15.4 (Leis de DeMorgan): $(10a)\ (a + b)' = a' * b'$ $\ (10b)\ (a * b)' = a' + b'$.

Demonstramos esses teoremas nos Problemas 15.6 e 15.7

15.5 ÁLGEBRAS BOOLEANAS E RETICULADOS

Segundo o Teorema 15.2 e o axioma $[\mathbf{B_1}]$, toda álgebra Booleana satisfaz as Leis Associativa, Comutativa e de Absorção e, portanto, é um reticulado em que $+$ e $*$ são as operações de união e interseção, respectivamente. Em relação a esse reticulado, $a + 1 = 1$ implica $a < 1$ e $a * 0 = 0$ implica $0 < a$ para qualquer elemento $a \in B$. Logo, B é um reticulado cotado. Além disso, os axiomas $[\mathbf{B_2}]$ e $[\mathbf{B_4}]$ mostram que B é também distributivo e complementado. Reciprocamente, todo reticulado L cotado, distributivo e complementado satisfaz os axiomas $[\mathbf{B_1}]$ até $[\mathbf{B_4}]$. Logo, temos o seguinte:

Definição alternativa: Uma álgebra Booleana B é um reticulado cotado, distributivo e complementado.

Uma vez que uma álgebra Booleana B é um reticulado, ela possui uma ordem parcial natural (e, portanto, seus diagramas podem ser desenhados). Lembre-se (Capítulo 14) de que definimos $a \leq b$ quando as condições equivalentes $a + b = b$ e $a * b = a$ são válidas. Uma vez que estamos em uma álgebra Booleana, podemos dizer muito mais:

Teorema 15.5: Os itens a seguir são equivalentes em uma álgebra Booleana.

$$(1)\ a + b = b, \quad (2)\ a * b = a, \quad (3)\ a' + b = 1, \quad (4)\ a * b' = 0$$

Logo, em uma álgebra Booleana, podemos escrever $a < b$ quando qualquer uma das quatro condições acima for verdadeira.

Exemplo 15.2

(a) Considere um conjunto de álgebras Booleanas. Então o conjunto A precede o conjunto B se A é um subconjunto de B. O Teorema 15.4 nos diz que, se $A \subseteq B$, então as condições a seguir são válidas

$$(1)\ A \cup B = B \quad (2)\ A \cap B = A \quad (3)\ A^C \cup B = \mathbf{U} \quad (4)\ A \cap B^C = \emptyset$$

(b) Considere a álgebra Booleana $\mathbf{D}_{70}$. Então a precede b se a divide b. Nesse caso, mmc$(a, b) = b$ e mdc$(a, b) = a$. Por exemplo, considere que $a = 2$ e $b = 14$ Então as condições a seguir são válidas:

(1) mmc$(2, 14) = 14$. (3) mmc$(2', 14) =$ mmc$(35, 14) = 70$.
(2) mdc$(2, 14) = 2$. (4) mdc$(2, 14') =$ mdc$(2, 5) = 1$.

15.6 TEOREMA DA REPRESENTAÇÃO

Seja B uma álgebra Booleana finita. Lembre (Seção 14.10) que um elemento a em B é um átomo se a sucede imeditamente 0, isto é, se $0 \ll a$ Sejam A um conjunto de átomos de B e $P(A)$ uma álgebra Booleana de todos os subconjuntos do conjunto A de átomos. Segundo o Teorema 14.8, cada $x \neq 0$ em B pode ser expressado unicamente (exceto pela ordem) como a soma (união) de átomos, isto é, elementos de A. Digamos,

$$x = a_1 + a_2 + \cdots + a_r$$

nessa representação. Considere a função $f: B \to P(A)$, definida por

$$f(x) = \{a_1, a_2, \ldots, a_r\}$$

O mapeamento é bem definido, uma vez que a representação é única.

Teorema 15.6: O mapeamento acima $f: B \to P(A)$ é um isomorfismo.

Logo, vemos a íntima relação entre teoria de conjuntos e álgebras Booleanas abstratas no sentido de que toda álgebra Booleana finita é estruturalmente igual a uma álgebra Booleana de conjuntos.

Se um conjunto A possui n elementos, então seu conjunto potência $P(A)$ possui 2^n elementos. Logo, o teorema acima nos dá nosso próximo resultado.

Corolário 15.7: Uma álgebra booleana finita possui 2^n elementos para algum inteiro positivo n.

Exemplo 15.3: Considere a álgebra Booleana $\mathbf{D}_{70} = \{1, 2, 5, \ldots, 70\}$, cujo diagrama nos é dado na Fig. 15-2(a). Note que $A = \{2, 5, 7\}$ é o conjunto de átomos de $\mathbf{D}_{70}$. A seguir temos a representação única de cada não átomo, usando átomos:

$$10 = 2 \vee 5, \quad 14 = 2 \vee 7, \quad 35 = 5 \vee 7, \quad 70 = 2 \vee 5 \vee 7$$

A Figura 15.2(b) nos dá o diagrama da álgebra Booleana do conjunto potência $P(A)$ do conjunto A de átomos. Observe que os dois diagramas são estruturalmente iguais.

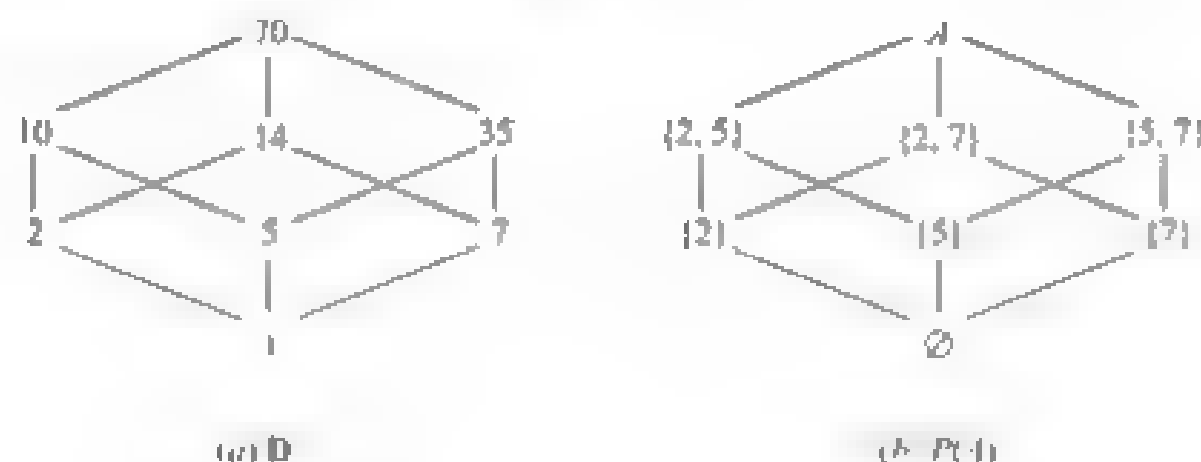



Figura 15-2

15.7 FORMA DE SOMA DE PRODUTOS PARA CONJUNTOS

Esta seção motiva o conceito da forma de soma de produtos na álgebra Booleana por meio de um exemplo de teoria de conjuntos. Considere o diagrama de Venn, na Fig. 15-3, de três onjuntos A, B e C. Observe que esses

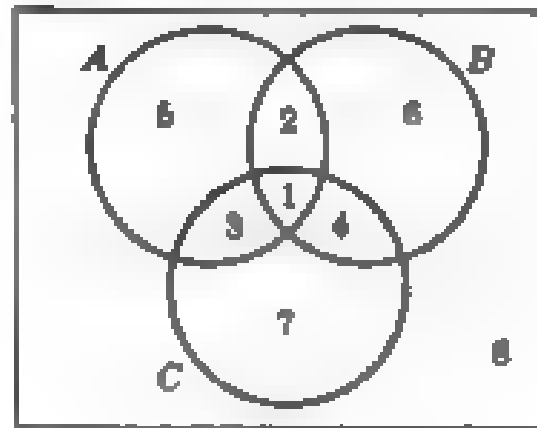



Figura 15-3

conjuntos particionam o retângulo (conjunto universal) em oito conjuntos numerados que podem ser representados como se segue:

(1) $A \cap B \cap C$ (3) $A \cap B^c \cap C$ (5) $A \cap B^c \cap C^c$ (7) $A^c \cap B^c \cap C$

(2) $A \cap B \cap C^c$ (4) $A^c \cap B \cap C$ (6) $A^c \cap B \cap C^c$ (8) $A^c \cap B^c \cap C^c$

Cada um desses oito conjuntos é da forma $A^* \cap B^* \cap C^*$, onde:

$$A^* = A \text{ ou } A^c, \quad B^* = B \text{ ou } B^c, \quad C^* = C \text{ ou } C^c$$

Considere qualquer expressão de conjunto não vazio R envolvendo os conjuntos A, B e C, digamos,

$$E = [(A \cap B^c)^c \cup (A^c \cap C^c)] \cap (B^c \cup C)^c \cap (A \cup C^c)]$$

Então E representará alguma área na Fig. 15-3 e, portanto, será unicamente igual à união de um ou mais dos oito conjuntos.

Suponha que, agora, interpretamos uma união como uma soma e uma interseção como um produto. Então os oito conjuntos acima são produtos e a representação única de E será uma soma (união) de produtos. Essa representação única de E é a mesma que a expansão de soma de produtos completa em álgebras Booleanas que discutimos abaixo.

15.8 FORMA DE SOMA DE PRODUTOS PARA ÁLGEBRAS BOOLEANAS

Considere um conjunto de variáveis (ou letras, ou símbolos), digamos $x_1, x_2, \ldots, x_n$. Uma *expressão Booleana E* nessas variáveis, às vezes escrita como $E(x_1, \ldots, x_n)$, é qualquer variável ou qualquer expressão construída a partir das variáveis usando as operações Booleanas $+$, $*$ e $'$ (Naturalmente, a expressão E deve ser *bem formada*, isto é, onde $+$ e $*$ são usados como operações binárias e $'$ é usada como operação unária.) Por exemplo,

$$E_1 = (x + y' z)' + (xyz' + x' y)' \quad \text{e} \quad E_2 = ((xy'z' + y)' + x' z)'$$

são expressões Booleanas em x, y e z.

Um *literal* é uma variável ou uma variável complementada, como x, x', y, y', e assim por diante. Um *produto fundamental* é um literal ou um produto de dois ou mais literais em que não existem dois literais envolvendo a mesma variável. Logo,

$$xz', \quad xy' z, \quad x, \quad y', \quad x'yz$$

são produtos fundamentais, mas $xyx' z$ e $xyzy$ não são. Note que qualquer produto de literais pode ser reduzido a 0 ou a um produto fundamental, por exemplo, $xyx' z = 0$, uma vez que $xx' = 0$ (Lei de Complemento) e $xyzy = xyz$, já que $yy = y$ (Lei da Idempotência).

Um produto fundamental P_1 se diz *contido em* (ou *incluído em*) outro produto fundamental P_2 se os literais de P_1 são também literais de P_2. Por exemplo, $x'z$ está contido em $x'yz$, mas $x'z$ não está contido em $xy'z$, uma vez que x' não é um literal de $xy'z$. Observe que, se P_1 está contido em P_2, digamos $P_2 = P_1 * Q$, então, segundo a Lei da Absorção,

$$P_1 + P_2 = P_1 + P_1 * Q = P_1$$

Então, por exemplo, $x'z + x'yz = x'z$.

Definição 15.1: Uma expressão Booleana E é chamada de expressão de *soma de produtos* se E é um produto fundamental ou a soma de dois ou mais produtos fundamentais que não estejam contidos em outro.

Definição 15.2: Seja E qualquer expressão Booleana. Uma *forma de soma de produtos* de E é uma expressão Booleana de soma de produtos equivalente.

Exemplo 15.4 Considere as expressões

$$E_1 = xz' + y'z + xyz' \text{ e } E_2 = xz' + x'yz' + xy'z$$

Apesar de a primeira expressão E_1 ser uma soma de produtos, ela não é uma expressão de soma de produtos. Especificamente, o produto xz' está contido no produto xyz'. Contudo, segundo a Lei da Absorção, E_1 pode ser expresso como

$$E_1 = xz' + y'z + xyz' = xz' + xyz' + y'z = xz' + y'z$$

Isso implica em uma forma de soma de produtos para E_1. A segunda expressão E_2 é, por sua vez, uma expressão de soma de produtos.

Algoritmo para encontrar formas de soma de produtos

A Figura 15-4 nos dá um algoritmo de quatro passos que usa leis da álgebra Booleana para transformar qualquer expressão Booleana em uma expressão de soma de produtos equivalente.

Algoritmo 15.1. A entrada é uma expressão Booleana E. A saída é uma expressão de soma de produtos equivalente a E.

Passo 1. Use as Leis de DeMorgan e Involução para mover a operação complementar para qualquer parêntese até que, finalmente, a operação complementar se aplique apenas a variáveis. Então E consistirá apenas em somas e produtos de literais.

Passo 2. Use a operação distributiva para transformar E em uma soma de produtos.

Passo 3. Use as Leis Comutativa, a Idempotência e de Complemento para transformar cada produto em E em 0 ou em um produto fundamental.

Passo 4. Use as Leis de Absorção e de Identidade para, finalmente, transformar E em uma expressão de soma de produtos.

Figura 15-4

Exemplo 15.5 Suponha que o Algoritmo 15.1 é aplicado à seguinte expressão Booleana:

$$E = ((xy)'z)'((x' + z)(y' + z'))'$$

Passo 1. Usando as Leis de DeMorgan e de Involução, obtemos

$$E = (xy'' + z')((x' + z)' + (y' + z')') = (xy + z')(xz' + yz)$$

E agora consiste apenas em somas e produtos de literais.

Passo 2. Usando as Leis Distributivas, obtemos

$$E = xyxz' + xyyz + xz'z' + yzz'$$

E, agora, é uma soma de produtos.

Passo 3. Usando as Leis Comutativa, da Idempotência e de Complemento, obtemos

$$E = xyz' + xyz + xz' + 0$$

Cada termo em E é um produto fundamental ou 0.

Passo 4. O produto xz' está contido em xyz'; logo, segundo a Lei de Absorção,

$$xz' + (xz'y) = xz'$$

Logo, podemos deletar xyz' da soma. Além disso, segundo a Lei de Identidade para 0, podemos deletar 0 da soma. Logo,

$$E = xyz + xz'$$

E é, agora, representado por uma expressão de soma de produtos.

Formas completas de soma de produtos

Uma expressão Booleana $E = E(x_1, x_2, \ldots, x_n)$ é dita uma expressão *de soma de produtos completa* se E é uma expressão de soma de produtos em que cada produto P envolve todas as n variáveis. Um produto fundamental P que envolve todas as variáveis é chamado de *mintermo* e existe um máximo de 2^n produtos para n variáveis. O seguinte teorema se aplica.

Teorema 15.8: Toda expressão Booleana diferente de zero $E = E(x_1, x_2, \ldots, x_n)$ é equivalente a uma expressão de soma de produtos completa e tal representação é única.

A representação única de E acima é chamada de *forma de soma de produtos completa* de E. O Algoritmo 15-1 na Fig. 15-4 nos diz como transformar E em uma forma de soma de produtos. A Figura 15-5 contém um algoritmo que transforma uma forma de soma de produtos em uma forma de soma de produtos completa.

Algoritmo 15.2: A entrada é uma expressão Booleana de soma de produtos $E = E(x_1, x_2, \ldots, x_n)$. A saída é uma expressão de soma de produtos completa equivalente a E.

Passo 1. Encontre um produto P em E que não envolve a variável x_i e multiplique P por $x_i + x_i'$, deletando qualquer produto repetido. (Isso é possível, uma vez que $x_i + x_i' = 1$ e $P + P = P$.)

Passo 2. Repita o Passo 1 até que cada produto P em E seja um mintermo, isto é, todo produto P envolva todas as variáveis.

Figura 15-5

Exemplo 15.6 Expresse $E(x, y, z) = x(y'z)'$ em sua forma de soma de produtos completa.

(a) Aplique o Algoritmo 15.1 em E, de modo que E seja representado por uma expressão de soma de produtos.

$$E = x(y'z)' = x(y + z') = xy + xz'$$

(b) Agora aplique o Algoritmo 15.2 para obter:

$$\begin{aligned} E &= xy(z + z') + xz'(y + y') = xyz + xyz' + xyz' + xy'z' \\ &= xyz + xyz' + xy'z' \end{aligned}$$

Agora E está representado por sua forma de soma de produtos completa.

Aviso: A terminologia nesta seção não foi padronizada. A forma de soma de produtos para uma expressão Booleana E também é chamada de *forma disjuntiva normal* de E. A forma de soma de produtos completa para E também é chamada de *forma disjuntiva normal completa*, de *forma disjuntiva canônica* ou de *forma mintermo canônica* de E.

15.9 EXPRESSÕES BOOLEANAS MÍNIMAS, IMPLICANTES PRIMOS

Existem várias maneiras de representar a mesma expressão Booleana E. Aqui, definimos e investigamos uma forma mínima de soma de produtos para E. Precisamos também definir e investigar implicantes primos de E, uma vez que a soma de produtos mínima envolve os referidos implicantes. Outras formas mínimas existem, mas suas investigações estão além do objetivo deste texto.

Soma de produtos mínima

Considere uma expressão Booleana de soma de produtos E. Seja E_L a notação do número de literais em E (contada de acordo com a multiplicidade) e considere que E_S denota o número de parcelas em E. Por exemplo, suponha que

$$E = xyz' + x'y't + xy'z't + x'yzt$$

Então, $E_L = 3 + 3 + 4 + 4 = 14$ e $E_S = 4$

Considere que E e F são expressões Booleanas de soma de produtos equivalentes. Dizemos que E é *mais simples* do que F se.

$$\text{(i) } E_L < F_L \text{ e } E_S \leq F_L \quad \text{ou} \quad \text{(ii) } E_L \leq F_L \text{ e } E_S < F_L$$

Dizemos que E é *mínimo* se não existem expressões de somas de produtos equivalentes que sejam mais simples que E. Notamos que pode existir mais do que uma expressão mínima de soma de produtos.

Implicantes primos

Um produto fundamental P é chamado de *implicante primo* de uma expressão Booleana E se

$$P + E = E$$

mas nenhum outro produto fundamental contido em P possui essa propriedade. Por exemplo, suponha que

$$E = xy' + xyz' + x'yz'$$

É possível mostrar (Problema 15.5) que:

$$xz' + E = E, \quad \text{mas} \quad x + E \neq E \quad \text{e} \quad z' + E \neq E$$

Logo, xz' é um implicante primo de E.

O seguinte teorema é válido.

Teorema 15.9: Uma forma mínima de soma de produtos para uma expressão Booleana E é uma soma de implicantes primos de E.

As subseções subsequentes nos dão um método para encontrar os implicantes primos de E baseado na noção do consenso de produtos fundamentais. Esse método pode, então, ser usado para encontrar uma forma mínima de soma de produtos para E. A Seção 15.12 nos dá uma método geométrico para encontrarmos tais implicantes primos.

Consenso de produtos fundamentais

Sejam P_1 e P_2 produtos fundamentais tais que, exatamente uma variável, digamos x_k, aparece sem complementar em P_1 ou P_2 e com complementar no outro. Então, o *consenso* de P_1 e P_2 é o produto (sem repetições) dos literais de P_1 e dos literais de P_2 depois que x_k e x'_k são deletados. (Não definimos o consenso de $P_1 = x$ e $P_2 = x'$.)

O lema a seguir (provado no Problema 15.19) se aplica.

Lema 15.10: Suponha que Q é o consenso de P_1 e P_2. Então $P_1 + P_2 + Q = P_1 + P_2$.

Exemplo 15.7 Encontre o consenso Q de P_1 e P_2, onde:

(a) $P_1 = xyz's$ e $P_2 = xy't$.

Delete y e y' e, então, multiplique os literais de P_1 e P_2 (sem repetição) para obter $Q = xz'st$

(b) $P_1 = xy'$ e $P_2 = y$.

Deletando y e y' implica $Q = x$.

(c) $P_1 = x'yz$ e $P_2 = x'yt$

Nenhuma variável aparece sem complementar em um dos produtos e complementada no outro. Logo, P_1 e P_2 não possui consenso.

(d) $P_1 = x'yz$ e $P_2 = xyz'$.

Tanto x quanto z aparecem complementados em um dos produtos e sem complementar no outro. Logo, P_1 e P_2 não possuem consenso.

Método de consenso para encontrar implicantes primos

A Figura 15-6 contém um algoritmo, chamado de *método de consenso*, que é usado para encontrar os implicantes primos de uma expressão Booleana E. O teorema a seguir nos dá a propriedade básica desse algoritmo.

Teorema 15.11. O método de consenso, eventualmente, irá parar, então, E será a soma de seus implicantes primos.

Algoritmo 15.3 (Método de consenso): A entrada é uma expressão Booleana $E = P_1 + P_2 + \cdots + P_m$ em que os P's são produtos fundamentais. A saída expressa E como uma soma de seus implicantes primos (Teorema 15.11).

Passo 1. Delete qualquer produto fundamental P_i que inclua qualquer outro produto fundamental P_j. (Permitido pela Lei da Absorção).

Passo 2. Adicione o consenso de quaisquer P_i e P_j, contanto que Q não inclua qualquer dos P's. (Permitido pelo Lema 15.10).

Passo 3. Repita o Passo 1 e/ou o Passo 2 até que nenhum dos dois possa ser aplicado.

Figura 15-6

Exemplo 15.8 Seja $E = xyz + x'z' + xyz' + x'y'z + x'yz'$. Então:

$E = xyz + x'z' + xyz' + x'y'z$	($x'yz'$ inclui $x'z'$)
$= xyz + x'y' + xyz' + x'y'z + xy$	(consenso de xyz e xyz')
$= x'z' + x'y'z + xy$	(xyz e xyz' incluem xy)
$= x'z' + x'y'z + xy + x'y'$	(consenso de $x'z'$ e $x'y'z$)
$= x'z' + xy + x'y'$	($x'y'z$ inclui $x'y'$)
$= x'z' + xy + x'y' + yz'$	(consenso de $x'z'$ e xy)

Agora, nenhum dos passos no método do consenso mudará E. Logo, E é a soma de seus implicantes primos, que aparece na última linha, isto é, $x'z'$, xy, $x'y'$ e yz'.

Encontrando uma forma mínima de soma de produtos

O método do consenso (Algoritmo 15.3) é usado para expressar uma expressão Booleana E como uma soma de todos os seus implicantes primos. A Figura 15-7 contém um algoritmo que usa a referida soma para encontrar uma forma mínima de soma de produtos para E

Algoritmo 15.4: A entrada é uma expressão Booleana $E = P_1 + P_2 + \cdots + P_m$ em que os P's são todos os implicantes primos de E. A saída expressa E como uma mínima soma de produtos.

Passo 1. Expresse cada implicante primo P como uma soma de produtos completa.

Passo 2. Delete, um por vez, os implicantes primos cujas parcelas aparecem entre as parcelas dos implicantes primos restantes.

Figura 15-7

Exemplo 15.9 Aplicamos o Algoritmo 15.4 para a seguinte expressão E que (segundo o Exemplo 15.8) é, agora, expressa como a soma de todos os seus implicantes primos.

$$E = x'z' + xy + x'y' + yz'$$

Passo 1. Expresse cada implicante primo de E como uma soma de produtos completa para obter:

$$x'z' = x'z'(y + y') = x'yz' + x'y'z'$$
$$xy = xy(z + z') = xyz + xyz'$$
$$x'y' = x'y'(z + z') = x'y'z + x'y'z'$$
$$yz' = yz'(x + x') = xyz' + x'yz'$$

Passo 2. As parcelas de $x'z'$ são $x'yz$ e $x'y'z'$ que aparecem entre as outras parcelas. Logo, delete $x'z'$ para obter

$$E = xy + x'y' + yz'$$

As parcelas de nenhum outro implicante primo aparecem entre as parcelas dos implicantes primos restantes e, portanto, essa é uma forma mínima de soma de produtos para E. Em outras palavras, nenhum dos implicantes primos restantes é *supérfluo*, isto é, nenhum pode ser deletado sem existir uma mudança em E.

15.10 PORTÕES LÓGICOS E CIRCUITOS

Circuitos lógicos (também chamados de *redes lógicas*) são estruturas construídas a partir de certos circuitos elementares chamados de *portões lógicos*. Cada circuito lógico pode ser visto como uma máquina L que contém um ou mais mecanismos de entrada e exatamente um mecanismo de saída. Cada mecanismo de entrada em L manda um sinal, especificamente, um *bit* (dígito binário).

$$0 \quad \text{ou} \quad 1$$

ao circuito L, e L, por sua vez, processa o conjunto de bits para levar a um bit de saída. Logo, uma sequência de n bits pode ser associada a cada um dos mecanismos de entrada e L processa as sequências de entrada um bit por vez para produzir uma sequência de saída de n bits. Primeiro, definimos os portões lógicos, depois investigamos os circuitos lógicos.

Portões lógicos

Existem três portões lógicos básicos que são descritos abaixo. Adotamos a convenção de que as linhas que entram no símbolo do portão a partir da esquerda são linhas de entrada e a única linha à direita é a de saída.

(a) ***Portão OR*** A Figura 15-8(a) mostra um portão OR com entradas A e B e saída $Y = A + B$, onde "adição" é definida pela "tabela verdade" na Fig. 15-8(b). Logo, a saída $Y = 0$ apenas quando as entradas $A = 0$ e $B = 0$. Tal portão OR pode possuir mais do que duas entradas. A Figura 15-8(c) mostra um portão OR com quatro

entradas, A, B, C e D, e saída $Y = A + B + C + D$. A saída $Y = 0$ se, e somente se, todas as entradas forem iguais a 0.

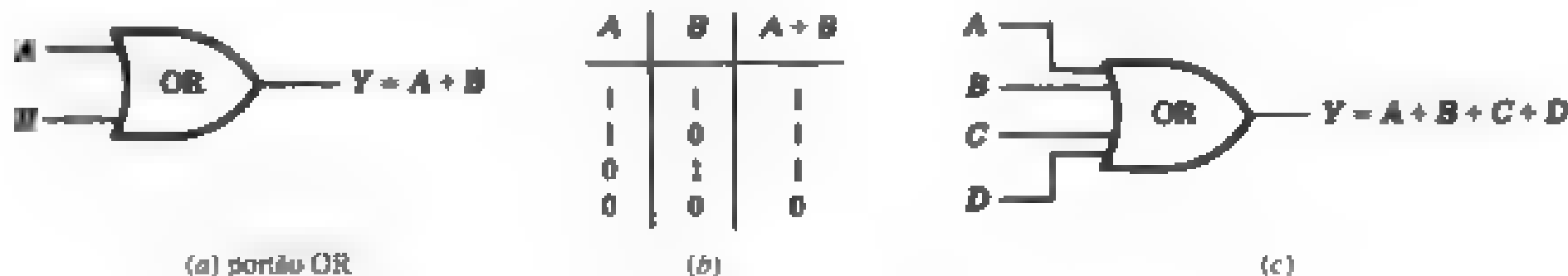
A	B	$A + B$
1	1	1
1	0	1
0	1	1
0	0	0

(a) portão OR (b) (c)

Figura 15-8

Suponha, por exemplo, que os dados de entrada para o portão OR na Fig. 15-5(c) são as seguintes sequências de 8 bits.

$$A = 10000101, \quad B = 10100001, \quad C = 00100100, \quad 10010101$$

O portão OR só implica 0 quando todos os bits de entrada são 0. Isso ocorre apenas na segunda, quinta e sétima posições (lendo da esquerda para a direita). Logo, a saída é a sequência $Y = 10110101$.

(b) ***Portão AND*** A Figura 15-9(a) mostra uma portão AND com entradas A e B e saída $Y = A \cdot B$ (ou, simplesmente, $Y = AB$)) onde "multiplicação" é definida pela "tabela verdade" na Fig. 15-9(b). Logo, a saída $Y = 1$ quando as entradas são $A = 1$ e $B = 1$, caso contrário, $Y = 0$. Tal portão AND pode possuir mais do que duas entradas. A Figura 15-9(c) mostra um portão AND com quatro entradas, A, B, C e D, e saída $Y = A \cdot B \cdot C \cdot D$. A saída $Y = 1$ se, e somente se, todas as entradas forem iguais a 1.

Suponha, por exemplo, que os dados de entrada para o portão AND na Fig. 15-9(c) são as seguintes sequências de 8 bits:

$$A = 11100111, \quad B = 01111011, \quad C = 01110011, \quad D = 11101110$$

O portão AND só implica 1 quando todos os bits de entrada são 1. Isso ocorre apenas na segunda, terceira e sétima posições. Logo, a saída é a sequência $Y = 01100010$.

A	B	$A \cdot B$
1	1	1
1	0	0
0	1	0
0	0	0

(a) portão AND (b) (c)

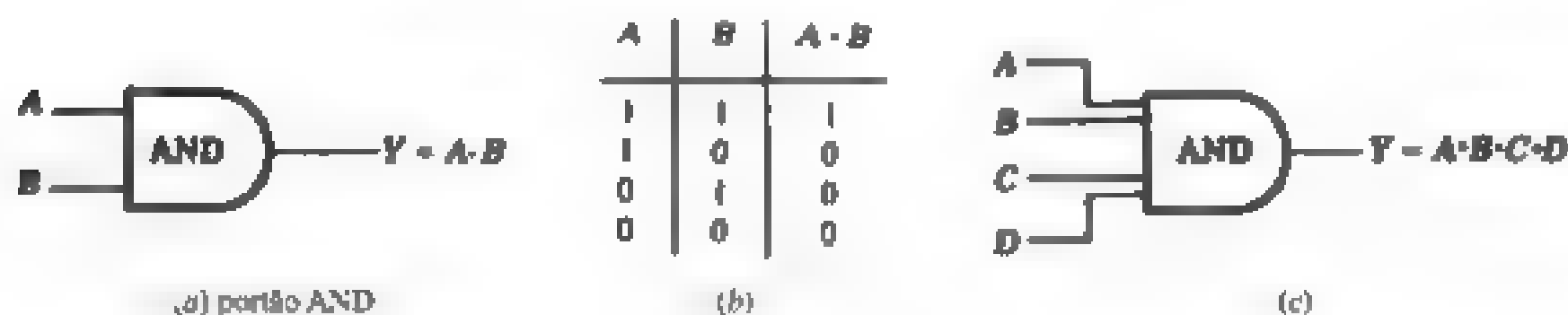



Figura 15-9

(c) ***Portão NOT*** A Figura 15-10(a) mostra um portão NOT, também chamado de *inversor*, com entrada A e saída $Y = A'$, onde a "inversão", denotada pelo primo, é definida pela "tabela verdade" na Fig. 15-10(b). O valor de saída $Y = A'$ é o oposto àquele da entrada A, isto é, $A' = 1$ quando $A = 0$ e $A' = 0$ quando $A = 1$. Enfatizamos que um portão NOT pode ter apenas uma entrada, enquanto que os portões OR e AND podem ter duas ou mais.

A	A'
1	0
0	1

(a) portão NOT (b)

Figura 15-10

Suponha, por exemplo, que um portão NOT é usado para processar as três sequências a seguir:

$$A_1 = 110001, \quad A_2 = 10001111, \quad A_3 = 101100111000$$

O portão NOT muda 0 para 1 e 1 para 0. Logo,

$$A'_1 = 001110, \quad A'_2 = 01110000, \quad A'_3 = 010011000111$$

são as três saídas correspondentes.

Circuitos lógicos

Um circuito lógico L é uma estrutura bem formada cujas componentes elementares são os referidos portões OR, AND e NOT. A Figura 15-11 é um exemplo de um circuito lógico com entradas A, B e C e saída Y. Um ponto indica um lugar em que a linha de entrada se divide de forma que seu sinal de bits é mandado para mais de uma direção. (Frequentemente, por uma questão de conveniência notacional, podemos omitir a palavra do interior do símbolo do portão.) Trabalhando da esquerda para a direita, expressamos Y em termos das entradas A, B e C como se segue. A saída do portão AND é $A \cdot B$, que é então negada para nos levar a $(A \cdot B)'$. A saída do portão OR inferior é $A' + C$, que é então negada para nos levar a $(A' + C)'$. A saída do portão OR à direita, com entradas $(A \cdot B)'$ e $(A' + C)'$, nos dá a representação desejada, isto é,

$$Y = (A \cdot B)' + (A' + C)'$$

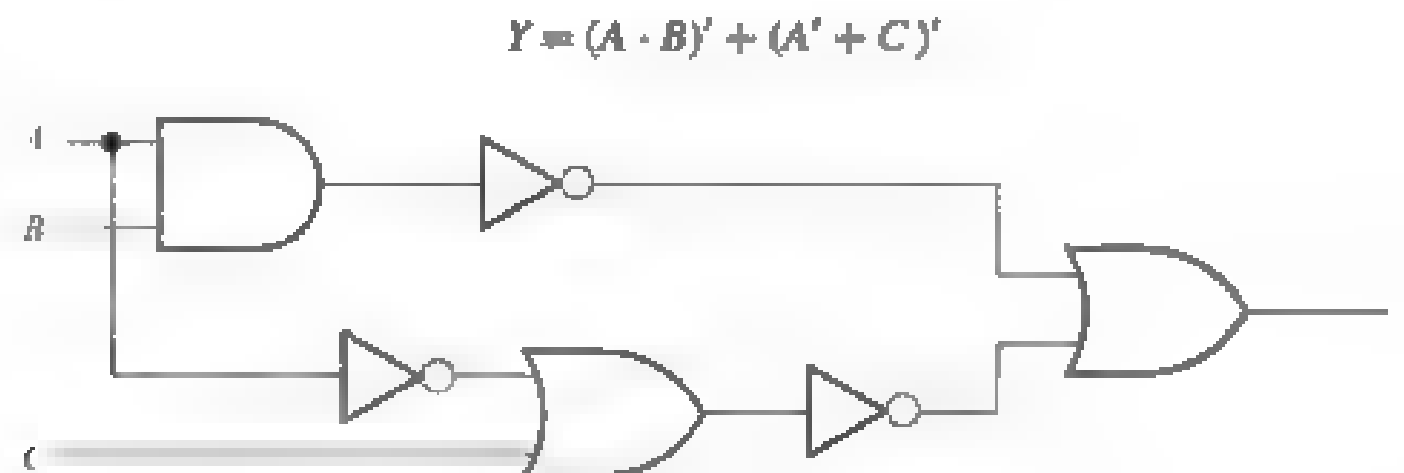



Figura 15-11

Circuitos lógicos como uma álgebra Booleana

Observe que as tabelas verdade para os portões OR, AND e NOT são respectivamente idênticas às tabelas verdade para as proposições $p \vee q$ (disjunção, "p ou q"), $p \wedge q$ (conjunção, "p e q"), e $\neg p$ (negação, "não p"), que aparece na Seção 4.3. A única diferença é a de que 1 e 0 são usados em vez de V e F. Logo, os circuitos lógios satisfazem as mesmas leis que proposições e, portanto, formam uma álgebra Booleana. Afirmamos esse resultado formalmente.

Teorema 15.12: Circuitos lógicos formam uma álgebra Booleana.

Logo, todos os termos usados em álgebras Booleanas como complementar, literais, produtos fundamentais, mintermos, soma de produtos e soma de produtos completa podem também ser usados com nossos circuitos lógicos.

Circuitos AND-OR

O circuito lógico L que corresponde a uma expressão Booleana de soma de produtos é chamado de circuito AND-OR. Tal circuito L possui várias entradas, em que:

(1) Algumas das entradas ou seus complementares são inseridos em cada portão AND.

(2) As saídas de todos os portões AND são inseridas em um único portão OR.

(3) A saída do portão OR é a saída do circuito L.

A seguir, uma ilustração desse tipo de circuito lógico.

Exemplo 15.10 A Figura 15-12 é um típico circuito AND-OR com três entradas, A, B e C, e saída Y. Podemos facilmente expressar Y como uma expressão Booleana nas entradas A, B e C como se segue. Primeiro, encontramos a saída de cada portão AND:

(a) As entradas do primeiro portão AND são A, B e C; logo, $A \cdot B \cdot C$ é a saída.

(b) As entradas do segundo portão *AND* são A, B' e C; logo, $A \cdot B' \cdot C$ é a saída.

(c) As entradas do terceiro portão AND são A' e B; logo, $A' \cdot B$ é a saída.

Então a soma das saídas dos portões AND é a saída do portão OR, que é a saída Y do circuito. Então:

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

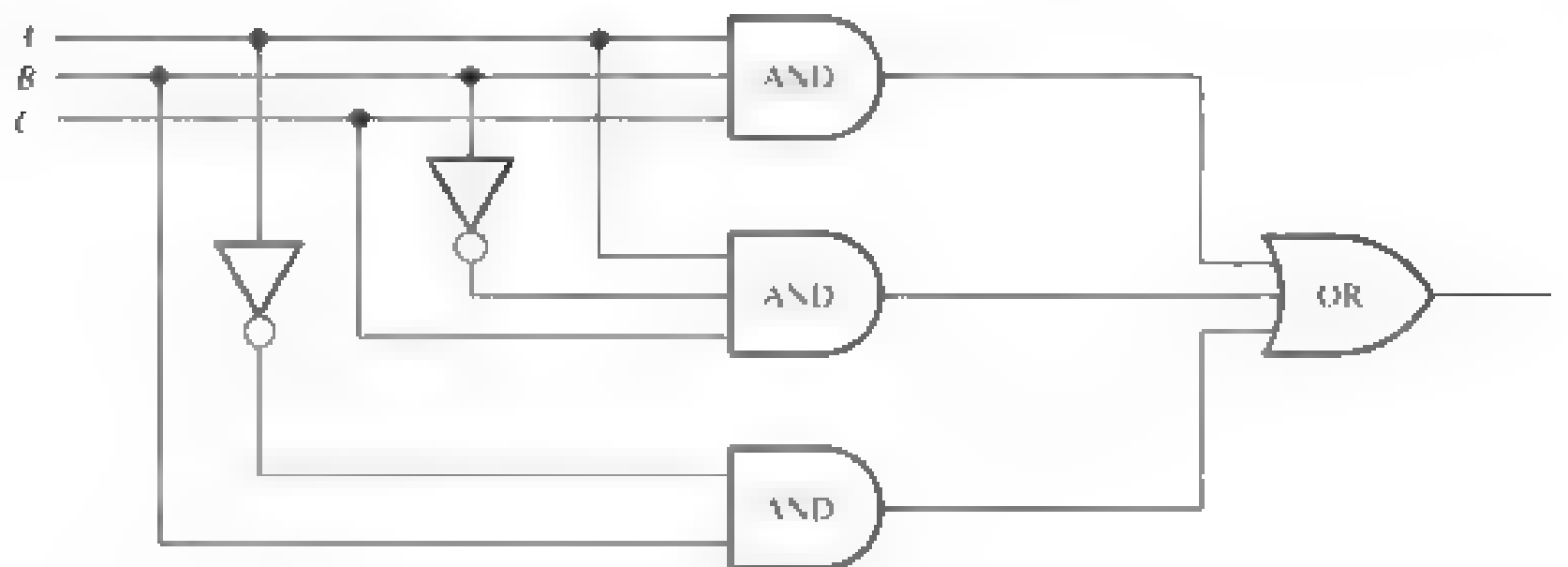



Figura 15-12

Portões NAND e NOR

Existem dois outros tipos de portões que são equivalentes a combinações dos portões básicos acima.

(a) Um portão NAND, ilustrado na Fig. 15-13(a), é equivalente a um portão AND seguido de um portão NOT.

(b) Um portão NOR, ilustrado na Fig. 15-13(b), é equivalente a um portão OR seguido de um portão NOT.

As tabelas verdade para esses portões (usando duas entradas A e B) aparecem na Fig. 15-13(c). Os portões NAND e NOR podem ter duas ou mais entradas, assim como seus portões correspondentes AND e OR. Além disso, a saída de um portão NAND é 0 se, e somente se, todas as entradas forem 1, e a saída de um portão NOR é 1 se, e somente se, todas as entradas forem 0.

A	B	NAND	NOR
1	1	0	0
1	0	1	0
0	1	1	0
0	0	1	1

(a) portão NAND (b) portão NOR (c)

Figura 15-13

Observe que a única diferença entre os portões AND e NAND e os portões OR e NOR é a de que os portões NAND e NOR são seguidos por um círculo. Alguns textos também usam um pequeno círculo para indicar um complementar antes de um portão. Por exemplo, as expressões Booleanas correspondendo a dois circuitos lógicos na Fig. 15-14 são listadas a seguir:

$$\text{(a)} \quad Y = (A' B)', \quad \text{(b)} \quad Y = (A' + B' + C)'$$

Figura 15-14

15.11 TABELAS VERDADE, FUNÇÕES BOOLEANAS

Considere um circuito lógico L com $n = 3$ dispositivos de entrada A, B e C e saída Y, digamos

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

Cada tarefa de um conjunto de três bits às entradas A, B e C implicam um bit de saída para Y. Existem, ao todo, $2^n = 2^3 = 8$ possíveis maneiras de executar os bits às entradas, como se segue:

$$000, 001, 010, 011, 100, 101, 110, 111$$

A pressuposição é a de que a sequência dos primeiros bits é associada a A, a sequência dos segundos bits é associada a B e a sequência dos terceiros bits a C. Logo, o conjunto acima de entradas pode ser reescrito na forma

$$A = 00001111, \quad B = 00110011, \quad C = 01010101$$

Enfatizamos que essas três $2^n = 8$-bit sequências contêm as oito possíveis combinações dos bits de entrada.

A *tabela verdade* $T = T(L)$ do circuito L acima consiste na sequência de saída Y que corresponde às sequências de entrada A, B e C. Essa tabela verdade T pode ser expressa usando notação fracional ou relacional, isto é, T pode ser reescrita na forma

$$T(A, B, C) = Y \quad \text{ou} \quad T(L) = [A, B, C; Y]$$

Essa forma para a tabela verdade para L é, essencialmente, a mesma que a tabela verdade para uma proposição, discutida na Seção 4.4. A única diferença é a de que aqui os valores para A, B, C e Y são escritos horizontalmente, sendo que, na Seção 4.4, a escrita é vertical.

Considere um circuito lógico L com n dispositivos de entrada. Existem várias maneiras de formar n sequências de entrada $A_1, A_2, \ldots, A_n$, de modo que elas contenham as 2^n possíveis combinações diferentes dos bits de entrada. (Note que cada sequência deve conter 2^n bits.) Um esquema de tarefas é apresentado a seguir:

A_1: Associe 2^{n-1} bits que são 0's, seguidos por 2^{n-1} que são 1's.

A_2: Associe repetidamente 2^{n-2} bits que são 0's, seguidos por 2^{n-2} bits que são 1's.

A_3: Associe repetidamente 2^{n-3} bits que são 0's, seguidos por 2^{n-3} bits que são 1's.

E assim por diante. As sequências obtidas dessa maneira serão chamadas de *sequências especiais*. Substituindo 0 por 1 e 1 por 0 nas sequências especiais implica os complementares dessas sequências.

Observação: Assumindo que a entrada é de sequências especiais, frequentemente dispensaremos a necessidade de distinguir entre a tabela verdade

$$T(L) = [A_1, A_2, \ldots, A_n, Y]$$

e a saída Y em si.

Exemplo 15.11

(a) Suponha que um circuito lógico L possui $n = 4$ dispositivos de entrada A, B, C e D. As $2^n = 2^4 = 16$-bit sequências especiais para A, B, C e D são listadas a seguir:

$$A = 0000000011111111, \quad C = 0011001100110011$$
$$B = 0000111100001111, \quad D = 0101010101010101$$

Isto é:

(1) A começa com oito 0's seguidos por oito 1's. (Aqui, $2^{n-1} = 2^3 = 8$.)

(2) B começa com quatro 0's seguidos por quatro 1's, e assim por diante. (Aqui, $2^{n-2} = 2^2 = 4$.)

(3) C começa com dois 0's seguidos por dois 1's, e assim por diante. (Aqui, $2^{n-3} = 2^1 = 2$.)

(4) D começa com um 0 seguido por um 1, e assim por diante. (Aqui, $2^{n-4} = 2^0 = 1$.)

(b) Suponha que um circuito lógico L possui $n = 3$ aparelhos de entrada A, B e C. As $2^n = 2^3 = 8$-bit sequências especiais para A, B e C e seus complementos A', B' e C' são listadas a seguir:

$$A = 00001111, \quad B = 00110011, \quad C = 01010101$$
$$A' = 11110000, \quad B' = 11001100, \quad C' = 10101010$$

A Figura 15-15 contém um algoritmo de três passos para encontrar a tabela verdade de um circuito lógico L em que a saída Y seja dada por uma expressão Booleana de soma de produtos nas entradas.

Algoritmo 15.5: A entrada é uma expressão Booleana de soma de produtos $Y = Y(A_1, A_2, \ldots)$.

Passo 1. Escreva as sequências especiais para as entradas $A_1, A_2, \ldots$ e seus complementos.

Passo 2. Encontre cada produto que aparece em Y. (Lembre-se de que um produto $X_1 \cdot X_2 \cdots = 1$ em uma posição se, e somente se, todos os $X_1, X_2, \ldots$ possuem 1 na posição.)

Passo 3. Encontre a soma Y dos produtos. (Lembre-se de que uma soma $X_1 + X_2 + \cdots = 0$ em uma posição se, e somente se, todos os $X_1, X_2, \ldots$ possuem 0 na posição.)

Figura 15-15

Exemplo 15.12 O Algoritmo 15.5 é usado para encontrar a tabela verdade $T = T(L)$ do circuito lógico L na Fig. 15-12 ou, de forma equivalente, das expressões booleanas de soma de produtos acima.

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

(1) As sequências especiais e seus complementos aparecem no Exemplo 15.14(*b*).

(2) Os produtos são os que seguem:

$$A \cdot B \cdot C = 00000001, \quad A \cdot B' \cdot C = 00000100, \quad A' \cdot B = 00110000$$

(3) A soma é $Y = 00110101$.

Logo,

$$T(00001111, 00110011, 01010101) = 00110101$$

ou, simplesmente, $T(L) = 00110101$ onde assumimos que a entrada consiste em sequências especiais.

Funções Booleanas

Seja E uma expressão Booleana com n variáveis $x_1, x_2, \ldots, x_n$. Toda a discussão pode ser aplicada a E em que, agora, as sequências especiais são associadas às variáveis $x_1, x_2, \ldots, x_n$ em vez dos dispositivos de entrada $A_1, A_2, \ldots, A_n$. A tabela verdade $T = T(E)$ de E é definida da mesma maneira que a tabela verdade $T = T(L)$ para um circuito lógico L. Por exemplo, a expressão Booleana

$$E = xyz + xy'z + x'y$$

que é análoga ao circuito lógico L no Exemplo 15.12, implica a tabela verdade

$$T(00001111, 00110011, 01010101) = 00110101$$

ou, simplesmente, $T(E) = 00110101$, em que assumimos que a entrada consiste nas sequências especiais.

Observação: A tabela verdade para uma expressão Booleana $E = E(x_1, x_2, \ldots, x_n)$ com n variáveis pode também ser vista como uma função "Booleana" de $\mathbf{B}^n$ em $\mathbf{B}$ (As álgebras Booleanas $\mathbf{B}^n$ e $\mathbf{B} = \{0, 1\}$ são definidas no Exemplo 15.1.) Isto é, cada elemento em $\mathbf{B}^n$ é uma lista de n bits em que, quando associados à lista de variáveis em E, produz um elemento em $\mathbf{B}$. A tabela verdade $T(E)$ de E é, simplesmente, o gráfico da função.

Exemplo 15.13

(a) Considere expressões Booleanas $E = E(x, y, z)$ com três variáveis. Os oito mintermos (produtos fundamentais envolvendo todas as três variáveis) são os que seguem.

$$xyz,\quad xyz',\quad xy'z,\quad x'yz,\quad xy'z',\quad x'yz',\quad x'y'z'$$

As tabelas verdade para esses mintermos (usando as sequências especiais para x, y e z) são as seguintes.

$$xyz = 00000001,\quad xyz' = 00000010,\quad xy'z = 00000100,\quad x'yz = 00001000$$
$$xy'z' = 00010000,\quad x'yz' = 00100000,\quad x'y'z = 01000000,\quad x'y'z' = 10000000$$

Observe que cada mintermo assume o valor 1 em apenas uma das oito posições.

(b) Considere a expressão Booleana $E = xyz' + x'yz + x'y'z$. Note que E é uma expressão de soma de produtos completa contendo três mintermos. Logo, a tabela verdade $T = T(E)$ para E, usando as sequências especiais para x, y e z, podem ser facilmente obtidas a partir das sequências da parte (a). Especificamente, a tabela verdade $T(E)$ irá conter exatamente três 1's na mesma posição que os 1's nos três mintermos em E. Logo,

$$T(00001111, 00110011, 01010101) = 01001010$$

ou, simplesmente, $T(E) = 01001010$.

15.12 MAPAS DE KARNAUGH

Mapas de Karnaugh, onde mintermos que envolvem as mesmas variáveis são representados por quadrados, são recursos pictóricos para encontrar implicantes primos e formas mínimas para expressões Booleanas envolvendo, no máximo, seis variáveis. Trataremos apenas os casos com duas, três e quatro variáveis. No contexto de mapas de Karnaugh, às vezes usaremos os termos "quadrados" e "mintermo" como sinônimos. Lembre-se de que um mintermo é um produto fundamental que envolve todas as variáveis e que uma expressão de soma de produtos completa é uma soma de mintermos.

Primeiro, precisamos definir a noção de produtos adjacentes. Dois produtos fundamentais P_1 e P_2 são ditos *adjacentes* se P_1 e P_2 possuem as mesmas variáveis e se diferem em, exatamente, um literal. Logo, precisa existir uma variável não complementada em um produto e complementada em outro. Em particular, a soma de dois produtos adjacentes será um produto fundamental com um literal a menos.

Exemplo 15.14 Encontre a soma dos produtos adjacentes P_1 e P_2, onde:

(a) $P = xyz'$ e $P_2 = xy'z'$.

$$P_1 + P_2 = xyz' + xy'z' = xz'(y + y') = xz'(1) = xz'$$

(b) $P_1 = x'yzt$ e $P_2 = x'yz't$.

$$P_1 + P_2 = x'yzt + x'yz't = x'yt(z + z') = x'yt(1) = x'yt$$

(c) $P_1 = x'yzt$ e $P_2 = xyz't$.

Aqui P_1 e P_2 não são adjacentes, uma vez que diferem em dois literais. Em particular,

$$P_1 + P_2 = x'yzt + xyz't = (x' + x)y(z + z')t = (1)y(1)t = yt$$

(d) $P_1 = xyz'$ e $P_2 = xyzt$

Aqui P_1 e P_2 não são adjacentes, uma vez que possuem variáveis diferentes. Logo, em particular, eles não aparecerão como quadrados no mesmo mapa de Karnaugh.

Caso de duas variáveis

O mapa de Karnaugh que corresponde a expressões Booleanas $E = E(x, y)$ com duas variáveis x e y é mostrado na Fig. 15-16(a). O mapa de Karnaugh pode ser visto como um diagrama de Venn onde x é representado pelos pontos na metade superior do mapa, sombreado na Fig. 15-16(b), e y é representado pelos pontos na metade esquerda do mapa, sombreado na Fig. 15-16(c). Logo, x' é representado pelos pontos na metade inferior do mapa e y' é representado pelos pontos na metade direita. Portanto, os quatro mintermos possíveis com dois literais,

$$xy, \quad xy', \quad x'y, \quad x'y'$$

são representados pelos quatro quadrados no mapa, como rotulados na Fig. 15-16(d). Obrserve que dois desses quadrados são adjacentes, como definido acima, se, e somente se, os quadrados forem geometricamente adjacentes (tiverem um lado em comum).

(a) (b) x sombreado (c) y sombreado (d)

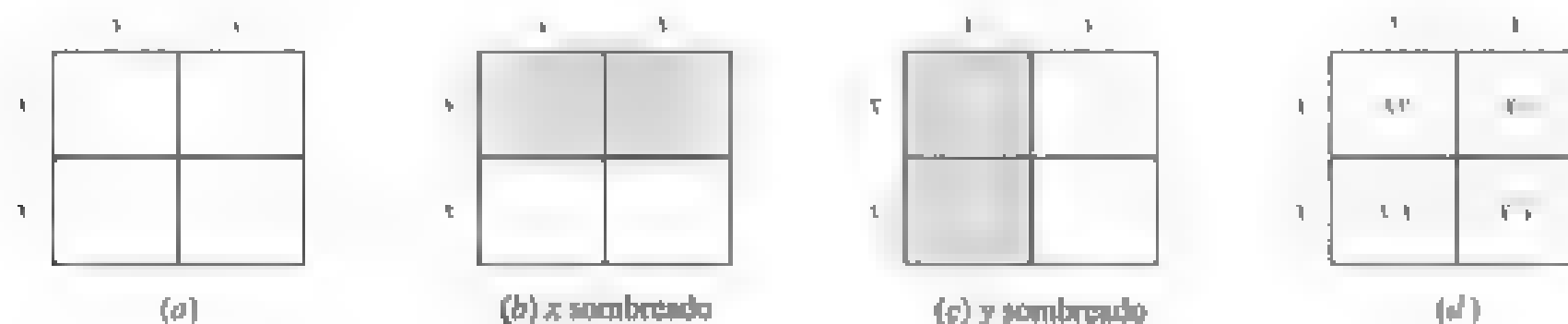



Figura 15-16

Qualquer expressão Booleana de soma de produtos completa $E(x, y)$ é uma soma de mintermos e, portanto, pode ser representada no mapa de Karnaugh, demarcando os quadrados apropriados. Um implicante primo de $E(x, y)$ será um par de quadrados adjacentes em E ou um quadrado *isolado*, isto é, um quadrado que não é adjacente a nenhum outro de $E(x, y)$. Uma forma mínima de soma de produtos para $E(x, y)$ consistirá em um número mínimo de implicantes primos que cobrem todos os quadrados de $E(x, y)$, como ilustrado no próximo exemplo.

Exemplo 15.15 Encontre os implicantes primos e uma forma mínima de soma de produtos para cada uma das expressões Booleanas de soma de produtos completa:

$$(a) \quad E_1 = xy + xy', \quad (b) \quad E_2 = xy + x'y + x'y'; \quad (c) \quad E_3 = xy + x'y'$$

Isso pode ser resolvido usando os mapas de Karnaugh como se segue:

(a) Marque os quadrados correspondendo a xy e xy', como ilustrado na Fig. 15-17(a). Note que E_1 consiste em um implicante primo, os dois quadrados adjacentes designados pela curva na Fig. 15-17(a). Esse par de quadrados adjacentes representa a variável x, então x é um (o único) implicante primo de E_1. Consequentemente, $E_1 = x$ é sua soma mínima.

(a) E_1 (b) E_2 (c) E_3

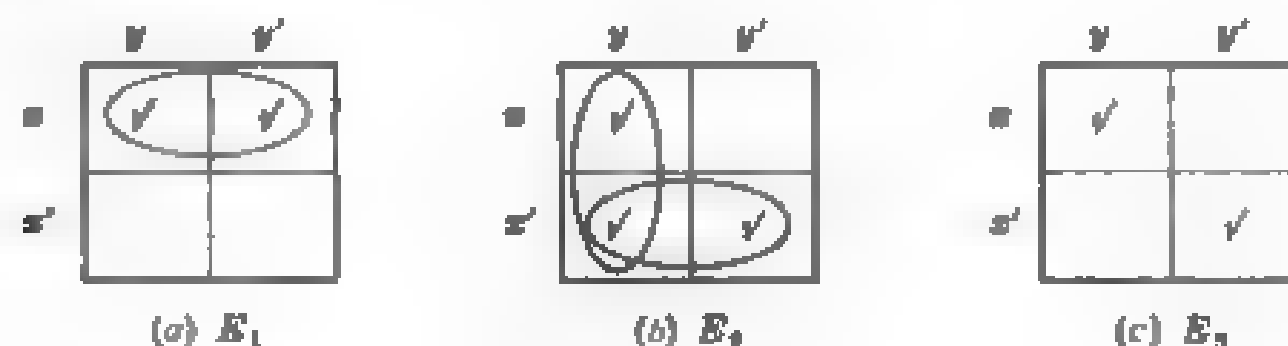



Figura 15-17

(b) Marque os quadrados correspondendo a xy, $x'y$ e $x'y'$ como na Fig. 15-17(b). Note que E_2 contém dois pares de quadrados adjacentes (designados pelas duas curvas) que incluem todos os quadrados de E_2. O par vertical representa y e o par horizontal representa x'; logo, y e x' são os implicantes primos de E_2. Portanto, $E_2 = x' + y$ é sua soma mínima.

(c) Marque os quadrados correspondendo a xy e $x'y'$ como na Fig. 15-17(c). Note que E_3 consiste em dois quadrados isolados que representam xy e $x'y'$; logo, xy e $x'y'$ são os implicantes primos de E_3 e $E_3 = xy + x'y'$ é sua soma mínima.

Caso de três variáveis

O mapa de Karnaugh correspondente às expressões Booleanas $E = E(x, y, z)$ com três variáveis x, y e z é mostrado na Fig. 15-18(a). Lembre-se de que existem exatamente oito mintermos com três variáveis.

$$xyz,\quad xyz',\quad xy'z',\quad xy'z,\quad x'yz,\quad x'yz',\quad x'y'z',\quad x'y'z$$

Esses mintermos são listados de modo que eles correspondam aos oito quadrados no mapa de Karnaugh de maneira óbvia.

Além disso, para que todo par de produtos adjacentes na Fig. 15-18(a) seja geometricamente adjacente, as arestas esquerda e direita do mapa devem ser identificadas. Isso é equivalente a cortar, entortar e colar o mapa ao longo das arestas identificadas para obter o cilindro que aparece na Fig. 15-18(b), onde produtos adjacentes são, agora, representados por quadrados com uma aresta em comum.

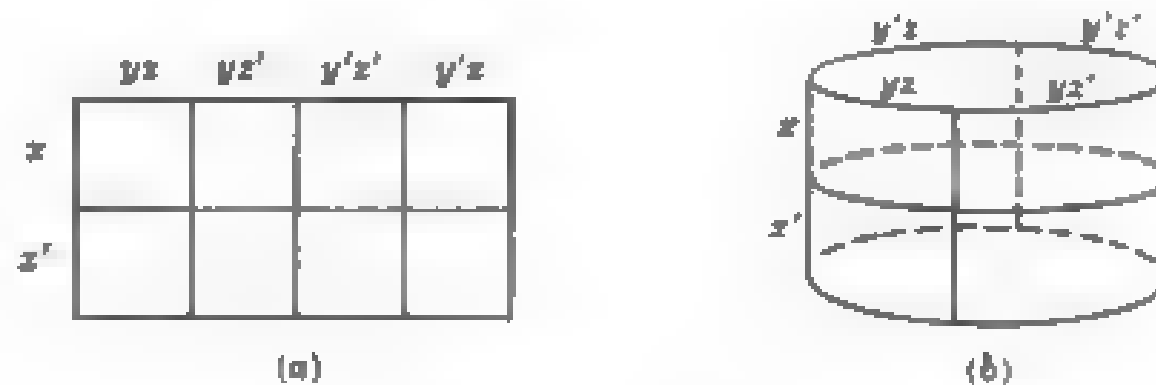



Figura 15-18

Vendo o mapa de Karnaugh na Fig. 15-18(a) como um diagrama de Venn, as áreas representadas pelas variáveis x, y e z são mostradas na Fig. 15-19. Especificamente, a variável x ainda é representada pelos pontos na metade superior do mapa, como está sombreado na Fig. 15-19(a), e a variável y ainda está representada pelos pontos na metade esquerda do mapa, como está sombreado na Fig. 15-19(b). A nova variável z é representada pelos pontos nos quartos esquerdo e direito do mapa, como está sombreado na Fig. 15-19(c). Logo, x', y' e z' são representados, respectivamente, pelos pontos na metade inferior, direita, e os dois quartos no meio do mapa.

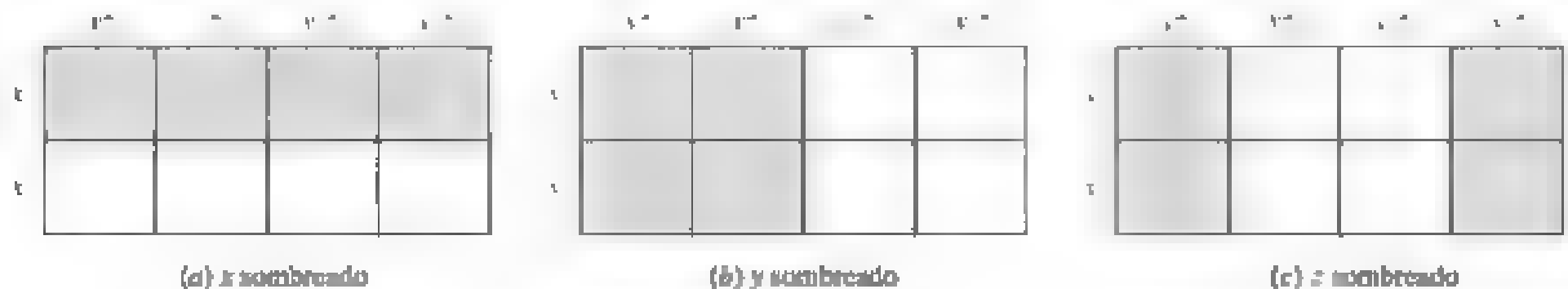



Figura 15-19

Quando falamos sobre um *retângulo básico* no mapa de Karnaugh com três variáveis, estamos nos referindo a um quadrado, dois quadrados adjacentes ou quatro quadrados que formem um retângulo de área um por quatro, ou dois por dois. Esses retângulos básicos correspondem a produtos fundamentais de três, dois e um literal, respecti-

vamente. Além disso, o produto fundamental representado por um retângulo básico é o produto desses mesmos literais que aparecem em todo quadrado do retângulo.

Suponha que uma expressão Booleana de soma de produtos completa $E = E(x, y, z)$ é representada pelo mapa de Karnaugh ao colocarmos marcações nos quadrados apropriados. Um implicante primo de E será um *retângulo básico máximo* de E, isto é, um retângulo básico contido em E que não está contido em nenhum outro retângulo básico maior em E. Uma forma mínima de soma de produtos para E consistirá em uma *cobertura mínima* de E, isto é, um número mínimo de retângulos básicos máximos de E que juntos incluem todos os quadrados de E.

Exemplo 15.16 Encontre os implicantes primos e uma forma mínima de soma de produtos para cada uma das expressões Booleanas de soma de produtos completa:

(a) $E_1 = xyz + xyz' + x'yz' + x'y'z$.

(b) $E_2 = xyz + xyz' + xy'z + x'yz + x'y'z$.

(c) $E_3 = xyz + xyz' + x'yz' + x'y'z' + x'y'z$.

Isso pode ser resolvido usando um mapa de Karnaugh como se segue:

(a) Marque os quadrados correspondendo às quatro parcelas, como na Fig. 15-20(a). Observe que E_1 possui três implicantes primos (retângulos básicos máximos), que estão circulados, esses são xy, yz' e $x'y'z$. Todos os três são necessários para cobrir E_1; logo, a soma mínima para E_1 é

$$E_1 = xy + yz' + x'y'z$$

(b) Marque os quadrados correspondentes às cinco parcelas, como na Fig. 15-20(b). Note que E_2 possui dois implicantes primos, que estão circulados. Um deles são os dois quadrados adjacentes que representam xy, o outro é o quadrado de área dois por dois (que percorre as arestas identificadas) que representa z. Ambos são necessários para cobrir E_2, então a soma mínima para E_2 é

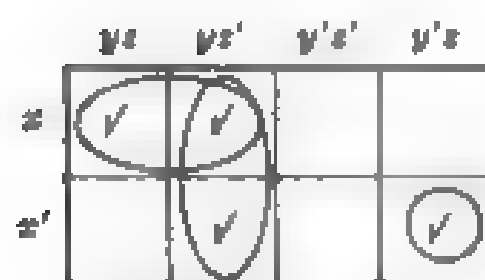
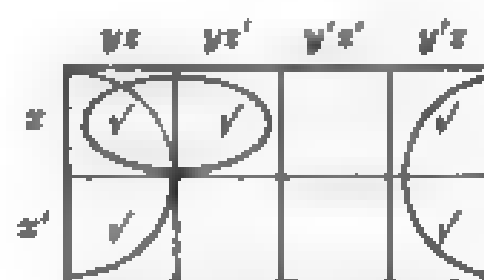
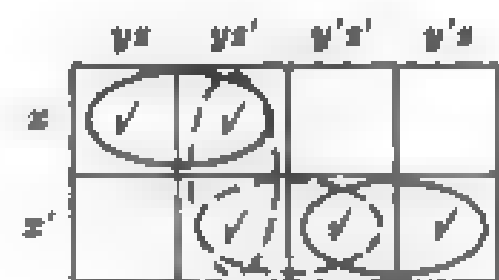
$$E_2 = xy + z$$

(a) E_1

(b) E_2

(c) E_3

Figura 15-20

(c) Marque os quadrados correspondendo às cinco parcelas, como na Fig. 15-20(c). Como indicado pelas curvas, E_3 possui quatro implicantes primos, xy, yz', $x'z'$ e $x'y'$. Contudo, apenas um dos dois marcados, isto é, um de yz' ou $x'z'$ é necessário em uma cobertura mínima de E_3. Logo, E_3 possui três somas mínimas

$$E_3 = xy + yz' + x'y' = xy + x'z' + x'y'$$

Exemplo 15.17 Desenhe um circuito mínimo L AND-OR, usando três entradas, usando a tabela verdade a seguir

$$T = [A, B, C; L] = [00001111, 00110011, 01010101; 11001101]$$

A partir da tabela verdade, podemos ler a forma de soma de produtos completa para L (como no Exemplo 15.10)

$$L = A'B'C' + A'B'C + AB'C' + AB'C + ABC$$

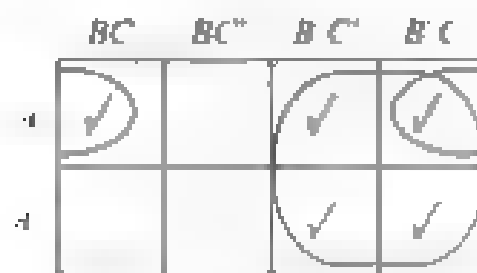
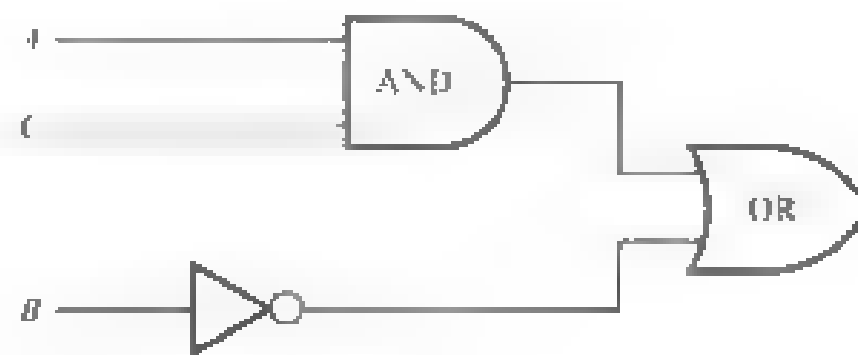
O mapa de Karnaugh associado é mostrado na Fig. 15-21(*a*). Observe que L possui dois implicantes primos, B' e AC, em sua cobertura mínima, logo, $L = B' + AC$ é uma soma mínima para L. A Figura 15-21(*b*) nos dá a correspondência do circuito mínimo L AND-OR.

(*a*) (*b*)

Figura 15-21

Caso de quatro variáveis

O mapa de Karnaugh correspondente a expressões Booleanas $E = E(x, y, z, t)$ com quatro variáveis x, y, z e t é mostrado na Fig. 15-22. Cada um dos 16 quadrados corresponde a um dos 16 mintermos com quatro variáveis,

$$xyzt, \quad xyzt', \quad xyz't', \quad xyz't, \quad \ldots, \quad x'yz't$$

como foi indicado pelas marcações de linha e coluna do quadrado. Observe que a linha superior e o lado esquerdo são demarcados de forma que os produtos adjacentes se diferenciem em, precisamente, um literal. Novamente, precisamos identificar a aresta esquerda com a direita (como fizemos com três variáveis), mas precisamos também identificar a aresta superior com a aresta inferior. (Essas identificações abrem portas a uma superfície em formato de anel chamada de *toroide*, e veremos nosso mapa como sendo, realmente, um toroide.)

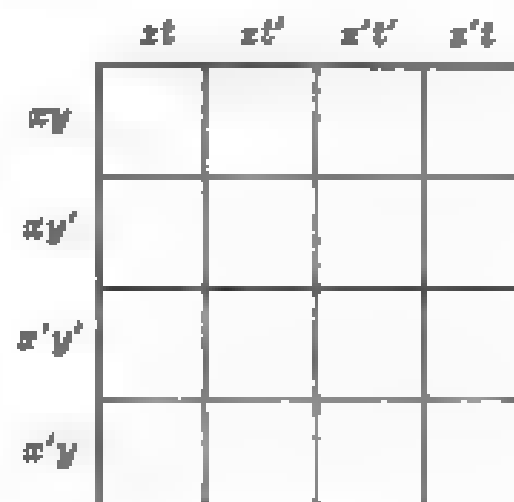



Figura 15-22

Um *retângulo básico* em um mapa de Karnaugh de quatro variáveis é um quadrado, dois quadrados adjacentes, quadrados a partir dos quais é formado um retângulo de área um por quatro ou dois por dois, ou oito quadrados que formam um retângulo de área dois por quatro. Esses retângulos correspondem a produtos fundamentais com quatro, três, dois e um literal, respectivamente. Novamente, retângulos básicos máximos são os implicantes primos. A técnica de minimização para uma expressão Booleana $E(x, y, z, t)$ é a mesma anterior.

Exemplo 15.18 Encontre o produto fundamental P representado pelo retângulo básico nos mapas de Karnaugh mostrados na Fig. 15-23.

Em cada caso, encontre os literais que aparecem em todos os quadrados do retângulo básico; P é o produto desses literais.

(a) xy e z' aparecem em ambos os quadrados; logo, $P = xyz'$.

(b) Apenas y e z aparecem em todos os quatro quadrados; logo, $P = yz$.
(c) Apenas t aparece em todos os oito quadrados; logo, $P = t$.

(a)

(b)

(c)

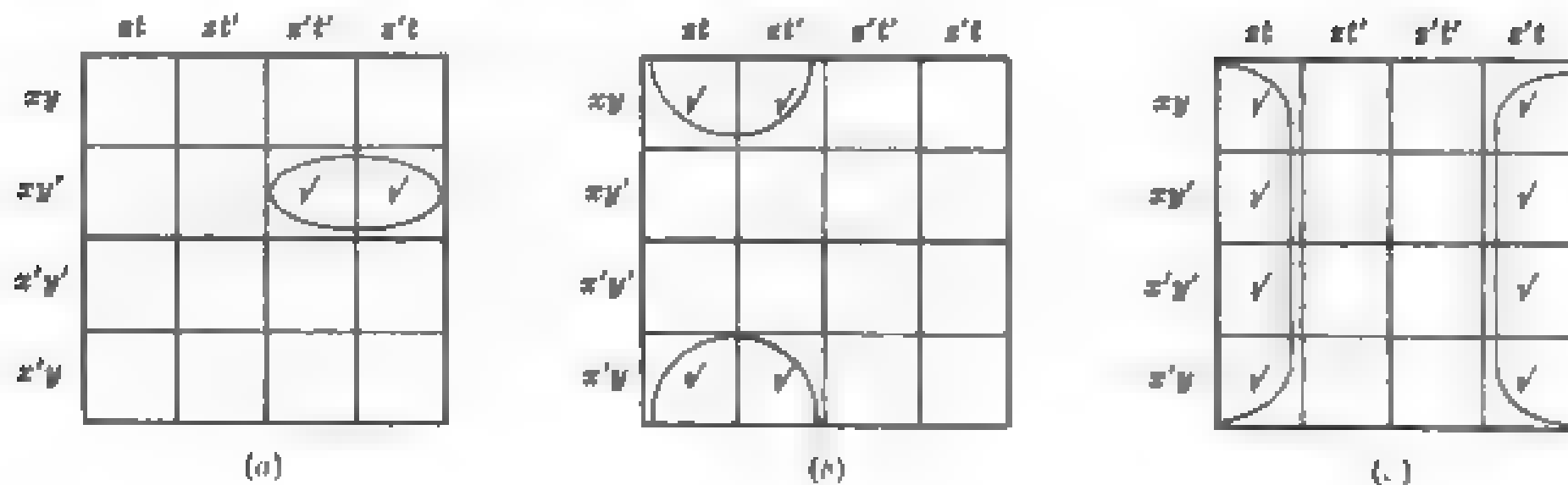



Figura 15-23

Exemplo 15.19 Use um mapa de Karnaugh para encontrar a forma mínima de soma de produtos para

$$E = xy' + xyz + x'y'z' + x'yzt'$$

Marque todos os quadrados representando cada produto fundamental. Isto é, marque todos os quatro quadrados representando xy', os dois quadrados representando xyz, os dois quadrados representando $x'y'z'$ e o quadrado representando $x'yzt'$, como na Fig. 15-24. Uma cobertura mínima do mapa consiste nos três retângulos básicos máximos designados.

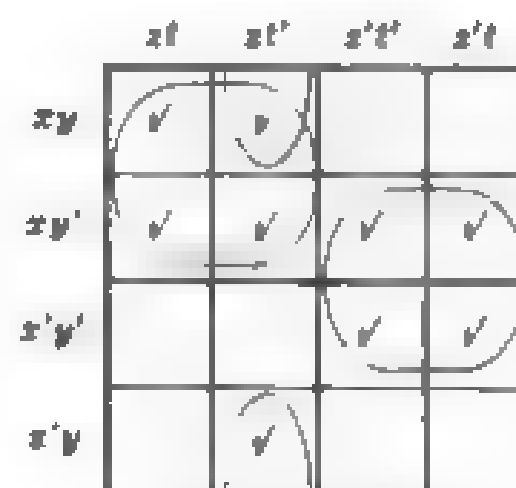



Figura 15-24

Os quadrados de área dois por dois representam os produtos fundamentais xz e $y'z'$ e os dois quadrados adjacentes (no topo e embaixo) representam yzt'. Logo,

$$E = xz + y'z' + yzt'$$

é uma soma mínima de E.

Problemas Resolvidos

Álgebras Booleanas

15.1 Escreva a dual de cada equação Booleana: (a) $(a * 1) * (0 + a') = 0$; (b) $a + a'b = a + b$.

(a) Para obter a equação dual, permute $+$ e $*$ e troque 0 e 1. Logo,

$$(a + 0) + (1 * a') = 1$$

(*b*) Primeiro, escreva a equação usando $*$ para obter $a + (a' * b) = a + b$. Então, a dual é $a * (a' + b) = a * b$, que pode ser escrito como

$$a(a' + b) = ab$$

15.2 Lembre-se (Capítulo 14) de que o conjunto $\mathbf{D}_m$ de divisores de m é um reticulado distributivo e cotado com

$$a + b = a \vee b = \text{mmc}(a, b) \quad \text{e} \quad a * b = a \wedge b = \text{mdc}(a, b).$$

(*a*) Mostre que $\mathbf{D}_m$ é uma álgebra Booleana se m é um quadrado livre, isto é, se m é um produto de primos distintos.

(*b*) Encontre os átomos de $\mathbf{D}_m$.

(*a*) Precisamos mostrar que $\mathbf{D}_m$ é complementado. Considere que x está em $\mathbf{D}_m$, e $x' = m/x$. Uma vez que m é um produto de primos distintos, x e x' possuem divisores primos diferentes. Logo, $x * x' = \text{mdc}(x, x') = 1$ e $x + x' = \text{mmc}(x, x') = m$. Lembre-se de que 1 é o elemento zero (limite inferior) de $\mathbf{D}_m$ e que m é o elemento identidade (limite superior) de $\mathbf{D}_m$. Logo, x' é um complemento de x e, portanto, $\mathbf{D}_m$ é uma álgebra Booleana.

(*b*) Os átomos de $\mathbf{D}_m$ são os divisores primos de m.

15.3 Considere a álgebra Booleana $\mathbf{D}_{210}$.

(*a*) Liste seus elementos e esboce seu diagrama.

(*b*) Encontre o conjunto A de átomos.

(*c*) Encontre duas subálgebras com oito elementos.

(*d*) $X = \{1, 2, 6, 210\}$ é um subreticulado de $\mathbf{D}_{210}$? Uma subálgebra?

(*e*) $Y = \{1, 2, 3, 6\}$ é um subreticulado de $\mathbf{D}_{210}$? Uma subálgebra?

(*a*) Os divisores de 210 são 1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105 e 210. O diagrama de $\mathbf{D}_{210}$ aparece na Fig. 15-25.

(*b*) $A = \{2, 3, 5, 7\}$, o conjunto de divisores primos de 210.

(*c*) $B = \{1, 2, 3, 35, 6, 70, 105, 210\}$ e $C = \{1, 5, 6, 7, 30, 35, 42, 210\}$ são subálgebras de $\mathbf{D}_{210}$.

(*d*) X é um subreticulado, uma vez que é linearmente ordenado. Contudo, X não é uma subálgebra, uma vez que 35 é o complementar de 2 em $\mathbf{D}_{210}$, mas 35 não pertence a X. (Na verdade, nenhuma álgebra Booleana com mais de dois elementos é linearmente ordenada.)

(*e*) Y é um subreticulado de $\mathbf{D}_{210}$, uma vez que ele é fechado sob $+$ e $*$. Contudo, Y não é uma subálgebra de $\mathbf{D}_{210}$, uma vez que não é fechado sob complementos em $\mathbf{D}_{210}$, por exemplo, $35 = 2'$ não pertence a Y. (Notamos que o próprio Y é uma álgebra Booleana, na verdade, $Y = D_6$.)

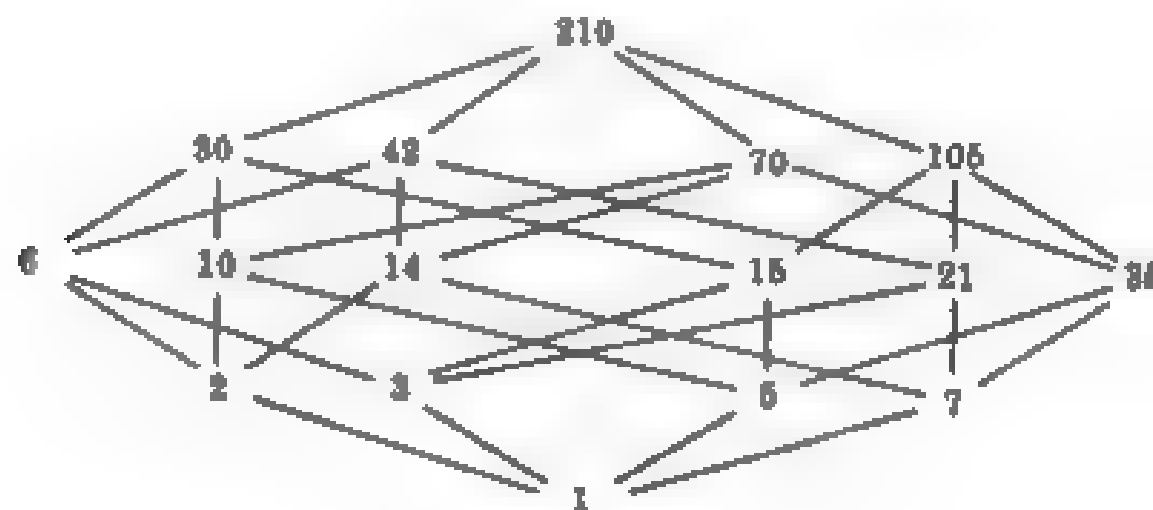



Figura 15-25

15.4 Encontre o número de subálgebras de $\mathbf{D}_{210}$.

Uma subálgebra de $\mathbf{D}_{210}$ deve conter dois, quatro, oito ou dezesseis elementos.

(i) Pode existir apenas uma subálgebra de dois elementos que consiste no limite suerior 210 e limite inferior 1, isto é, $\{1, 210\}$.

(ii) Uma vez que $\mathbf{D}_{210}$ contém dezesseis elementos, a única subálgebra com essa quantia de elementos é $\mathbf{D}_{210}$ em si.

(iii) Qualquer subálgebra de quatro elementos está na forma $\{1, x, x', 210\}$, isto é, consiste nos limites superior e inferior e em um elemento sem limite e seu complementar. Existem quatorze elementos sem limites em $\mathbf{D}_{210}$ e, portanto, existem $14/2 = 7$ pares $\{x, x'\}$. Logo, $\mathbf{D}_{210}$ possui sete subálgebras de oito elementos.

(iv) Qualquer subálgebra S de oito elementos conterá três átomos s_1, s_2, s_3. Podemos escolher s_1 e s_2 como quaisquer dois dos quatro átomos de $\mathbf{D}_{210}$ e, então, s_3 deve ser o produto dos outros dois átomos. Por exemplo, podemos ter $s_1 = 2, s_2 = 3, s_3 = 5 \cdot 7 = 35$ (que determina a subálgebra B acima) ou podemos ter $s_1 = 5, s_2 = 7, s_3 = 2 \cdot 3 = 6$ (que determina a subálgebra C acima). Existem $\binom{4}{2} = 6$ maneiras de escolher s_1 e s_2 a partir dos quatro átomos de $\mathbf{D}_{210}$ e, portanto, $\mathbf{D}_{210}$ tem seis subálgebras de oito elementos.

Logo, $\mathbf{D}_{210}$ possui $1 + 1 + 7 + 6 = 15$ subálgebras.

15.5 Demonstre o Teorema 15.2. Seja a, b e c quaisquer elementos em uma álgebra Booleana B.

(i) Leis de Idempotência:
$(5a)$ $a + a = a$ $\quad$ $(5b)$ $a * a = a$

(ii) Leis de Limites:
$(6a)$ $a + 1 = 1$ $\quad$ $(6b)$ $a * 0 = 0$

(iii) Leis de Absorção:
$(7a)$ $a + (a * b) = a$ $\quad$ $(7b)$ $a * (a + b) = a$

(iv) Leis Associativas:
$(8a)$ $(a + b) + c = a + (b + c)$ $\quad$ $(8b)$ $(a * b) * c = a * (b * c)$

$(5b)$ $a = a * 1 = a * (a + a') = (a * a) + (a * a') = (a * a) + 0 = a * a$

$(5a)$ Segue de $(5b)$ e do Princípio de Dualidade.

$(6b)$ $a * 0 = (a * 0) + 0 = (a * 0) + (a * a') = a * (0 + a') = a * (a' + 0) = a * a' = 0$

$(6a)$ Segue de $(6b)$ e do Princípio de Dualidade.

$(7b)$ $a * (a + b) = (a + 0) * (a + b) = a + (0 * b) = a + (b * 0) = a + 0 = a$

$(7a)$ Segue de $(7b)$ e do Princípio de Dualidade.

$(8b)$ Seja $L = (a * b) * c$ e $R = a * (b * c)$. Precisamos provar que $L = R$. Primeiro provamos que $a + L = a + R$. Usando as Leis de Absorção nos últimos dois passos,

$$a + L = a + ((a * b) * c) = (a + (a * b)) * (a + c) = a * (a + c) = a$$

Além disso, usando a Lei de Absorção no último passo,

$$a + R = a + (a * (b * c)) = (a + a) * (a + (b * c)) = a * (a + (b * c)) = a$$

Logo, $a + L = a + R$. A seguir, mostramos que $a' + L = a' + R$. Temos

$$\begin{aligned} a' + L &= a' + ((a * b) * c) = (a' + (a * b)) * (a' + c) \\ &= ((a' + a) * (a' + b)) * (a' + c) = (1 * (a' + b)) * (a' + c) \\ &= (a' + b) * (a' + c) = a' + (b * c) \end{aligned}$$

Além disso,

$$\begin{aligned} a' + R &= a' + (a * (b * c)) = (a' + a) * (a' + (b * c)) \\ &= 1 * (a' + (b * c)) = a' + (b * c) \end{aligned}$$

Logo, $a' + L = a' + R$. Consequentemente,

$$\begin{aligned} L &= 0 + L = (a * a') + L = (a + L) * (a' + L) = (a + R) * (a' + R) \\ &= (a * a') + R = 0 + R = R \end{aligned}$$

$(8a)$ Segue de $(8b)$ e do Princípio de Dualidade.

15.6 Demonstre o Teorema 15.3: Seja a qualquer elemento de uma álgebra Booleana B.

(i) (Unicidade de Complemento) Se $a + x = 1$ e $a * x = 0$, então $x = a'$.

(ii) (Lei de Involução) $(a')' = a$

(iii) (9a) $0' = 1$; (9b) $1' = 0$.

(i) Temos:

$$a' = a' + 0 = a' + (a * x) = (a' + a) * (a' + x) = 1 * (a' + x) = a' + x$$

Além disso,

$$x = x + 0 = x + (a * a') = (x + a) * (x + a') = 1 * (x + a') = x + a'$$

Logo, $x = x + a' = a' + x = a'$

(ii) Segundo a definição de complementar, $a + a' = 1$ e $a * a' = 0$. Por comutatividade, $a' + a = 1$ e $a' * a = 0$. Por Unicidade de Complemento, a é o complementar de a', isto é, $a = (a')'$.

(iii) Segundo a Lei de Limites (6a), $0 + 1 = 1$ e, segundo o axioma de identidade (3b), $0 * 1 = 0$. Por Unicidade de Complemento, 1 é o complementar de 0, isto é, $1 = 0'$. Por dualidade, $0 = 1'$.

15.7 Demonstre o Teorema 15.4: (Leis de DeMorgan) (10a) $(a + b)' = a' * b'$. (10b) $(a * b)' = a' + b'$

(10a) Precisamos mostrar que $(a + b) + (a' * b') = 1$ e $(a + b) * (a' * b') = 0$, então, por Unicidade de Complemento, $a' * b' = (a + b')$. Temos.

$$(a + b) + (a' * b') = b + a + (a' * b') = b + (a + a') * (a + b')$$
$$= b + 1 * (a + b') = b + a + b' = b + b' + a = 1 + a = 1$$

Além disso,

$$(a + b) * (a' * b') = ((a + b) * a') * b'$$
$$= ((a * a') + (b * a')) * b' = (0 + (b * a')) * b'$$
$$= (b * a') * b' = (b * b') * a' = 0 * a' = 0$$

Logo, $a' * b' = (a + b)'$

(10b) Princípio de Dualidade (Teorema 15.1).

15.8 Demonstre o Teorema 15.5. Os itens a seguir são equivalentes em uma álgebra Booleana:

(1) $a + b = b$; (2) $a * b = a$; (3) $a' + b = 1$; (4) $a * b' = 0$.

Segundo o Teorema 14.4, (1) e (2) são equivalentes. Mostramos que (1) e (3) são equivalentes. Suponha que (1) é válido. Então

$$a' + b = a' + (a + b) = (a' + a) + b = 1 + b = 1$$

Agora suponha que (3) é válido. Então

$$a + b = 1 * (a + b) = (a' + b) * (a + b) = (a' * a) + b = 0 + b = b$$

Logo, (1) e (3) são equivalentes.

A seguir mostramos que (3) e (4) são equivalentes. Suponha que (3) é válido. Segundo as Lei de DeMorgan e a de Involução,

$$0 = 1' = (a' + b)' = a'' * b' = a * b'$$

Reciprocamente, se (4) é válido, então

$$1 = 0' = (a * b')' = a' + b'' = a' + b$$

Logo, (3) e (4) são equivalentes. Portanto, todos os quatro são equivalentes.

15.9 Demonstre o Teorema 15.6: O mapeamento $f : B \to P(A)$ é o isomorfismo onde B é uma álgebra Booleana, $P(A)$ é o conjunto potência do conjunto A de átomos, e

$$f(x) = \{a_1, a_2, \ldots, a_n\}$$

onde $x = a_1 + \cdots + a_n$ é a representação única de a como sua soma de átomos.

Lembre-se (Capítulo 14) de que, se os a's são átomos, então $a_i^2 = a_i$, mas $a_i a_j = 0$ para $a_i \neq a_j$. Suponha que x e y estão em B e que

$$x = a_1 + \cdots + a_r + b_1 + \cdots + b_s$$
$$y = b_1 + \cdots + b_s + c_1 + \cdots + c_t$$

onde

$$A = \{a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_t, d_1, \ldots, d_k\}$$

é o conjunto de átomos de B. Então

$$x + y = a_1 + \cdots + a_r + b_1 + \cdots + b_s + c_1 + \cdots + c_t$$
$$xy = b_1 + \cdots b_s$$

Logo,

$$f(x + y) = \{a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_t\}$$
$$= \{a_1, \ldots, a_r, b_1, \ldots, b_s\} \cup \{b_1, \ldots, b_s, c_1, \ldots, c_t\}$$
$$= f(x) \cup f(y)$$
$$f(xy) = \{b_1, \ldots, b_s\}$$
$$= \{a_1, \ldots, a_r, b_1, \ldots, b_s\} \cap \{b_1, \ldots, b_s, c_1, \ldots, c_t\}$$
$$= f(x) \cap f(y)$$

Seja

$y = c_1 + \cdots + c_t + d_1 + \cdots + d_k$. Então $x + y = 1$ e $xy = 0$ e, portanto $y = x'$

Logo,

$$f(x') = \{c_1, \ldots, c_t, d_1, \ldots, d_k\} = \{a_1, \ldots, a_r, b_1, \ldots, b_s\}^c = (f(x))^c$$

Uma vez que a representação é única, f é um para um e sobrejetora. Portanto, f é um isomorfismo entre álgebras Booleanas.

Expressões Booleanas

15.10 Reduza os seguintes produtos Booleanos a 0 ou a um produto fundamental.

(*a*) $xyx'z$; (*b*) $xyzy$; (*c*) $xyz'yx$; (*d*) $xyz'yx'z$.

Use a Lei Comutativa $x * y = y * x$, a Lei de Complemento $x * x' = 0$ e a Lei da Idempotência $x * x = x$.

(*a*) $xyx'z = xx'yz = 0yz = 0$

(*b*) $xyzy = xyyz = xyz$

(*c*) $xyz'yx = xxyyz' = xyz'$

(*d*) $xyz'yx'z' = xx'yyz'z' = 0yz' = 0$

15.11 Expresse cada expressão Booleana $E(x, y, z)$ como uma soma de produtos e, então, na sua respectiva forma de soma de produtos completa: (*a*) $E = x(xy' + x'y + y'z)$; (*b*) $E = z(x' + y) + y'$.

Primeiro, use o Algoritmo 15.1 para expressar E como uma soma de produtos, depois, use o Algoritmo 15.2 para expressar E como uma soma de produtos completa.

(*a*) Primeiro, temos $E = xxy' + xx'y + xy'z = xy' + xy'z$. Então

$$E = xy'(z + z') + xy'z = xy'z + xy'z' + xy'z = xy'z + xy'z'$$

(*b*) Primeiro, temos

$$E = z(x' + y) + y' = x'z + yz + y'$$

Então

$$\begin{aligned} E &= x'z + yz + y' = x'z(y + y') + yz(x + x') + y'(x + x')(z + z') \\ &= x'yz + x'y'z + xyz + x'yz + xy'z + xy'z' + x'y'z + x'y'z' \\ &= xyz + xy'z + xy'z' + x'yz + x'y'z + x'y'z' \end{aligned}$$

15.12 Expresse $E(x, y, z) = (x' + y)' + x'y$ em sua forma de soma de produtos completa.

Temos $E = (x' + y)' + x'y = xy' + x'y$, que seria uma forma de soma de produtos completa de E se E fosse uma expressão Booleana em x e y. Contudo, é especificado que E é uma expressão Booleana nas três variáveis x, y e z. Logo,

$$E = xy' + x'y = xy'(z + z') + x'y(z + z') = xy'z + xy'z' + x'yz + x'yz'$$

é a forma de soma de produtos completa de E.

15.13 Expresse cada expressão Booleana $E(x, y, z)$ como uma soma de produtos e, então, em sua forma de soma de produtos completa: (*a*) $E = y(x + yz)'$; (*b*) $E = x(xy + y' + x'y)$.

(*a*) $E = y(x'(yz)') = yx'(y' + z') = yx'y' + x'yz' = x'yz'$, que já está em sua forma de soma de produtos completa.

(*b*) Primeiro, temos $E = xxy + xy' + xx'y = xy + xy'$. Então

$$E = xy(z + z') + xy'(z + z') = xyz + xyz' + xy'z + xy'z'$$

15.14 Expresse cada expressão conjuntista $E(A, B, C)$ envolvendo os conjuntos A, B e C como uma união de interseções:

(*a*) $E = (A \cup B)^C \cap (C^C \cup B)$; (*b*) $E = (B \cap C)^C \cap (A^C \cap C)^C$

Use a notação Booleana, ' para complementar, + para união e * (ou justaposição) para interseção e, então, expresse E como uma soma de produtos (união de interseções).

(*a*) $E = (A + B)'(C' + B) = A'B'(C' + B) = A'B'C' + A'B'B = A'B'C'$ ou $E = A^C \cap B^C \cap C^C$

(*b*) $E = (BC)'(A' + C)' = (B' + C')(AC') = AB'C' + AC'$ ou $E = (A \cap B^C \cap C^C) \cup (A \cap C^C)$

15.15 Seja $E = xy' + xyz' + x'yz'$. Prove que (*a*) $xz' + E = E$; (*b*) $x + E \neq E$; (*c*) $z' + E \neq E$.

Uma vez que a forma de soma de produtos completa é única, $A + E = E$, onde $A \neq 0$ se, e somente se, as parcelas na forma de soma de produtos completa para A estão entre as parcelas da forma de soma de produtos completa para E. Logo, encontre, em primeiro lugar, a forma de soma de produtos completa para E.

$$E = xy'(z + z') + xyz' + x'yz' = xy'z + xy'z' + xyz' + x'yz'$$

(*a*) Expresse xz' na forma de soma de produtos completa:

$$xz' = xz'(y + y') = xyz' + xy'z'$$

Uma vez que as parcelas de xz' estão entre as de E, temos $xz' + E = E$

(*b*) Expresse x na forma de soma de produtos completa.

$$x = x(y + y')(z + z') = xyz + xyz' + xy'z + xy'z'$$

A parcela xyz de x não é uma parcela de E; logo, $x + E \neq E$.

(*c*) Expresse z' na forma de soma de produtos completa:

$$z' = z'(x + x')(y + y') = xyz' + xy'z' + x'yz' + x'y'z'$$

A parcela $x'y'z'$ de z' não é uma parcela de E; logo, $z' + E \neq E$.

Expressões Booleanas mínimas, implicantes primos

15.16 Para qualquer expressão Booleana de soma de produtos E, assumimos que E_L denota o número de literais em E (contando a multiplicidade) e E_S denota o número de parcelas em E. Encontre E_L e E_S para cada um dos seguintes:

(*a*) $E = xy'z + x'z' + yz' + x$ (*c*) $E = xyt' + x'y'zt + xz't$

(*b*) $E = x'y'z + xyz + y + yz' + x'z$ (*d*) $E = (xy' + z)' + xy'$

Apenas some o número de literais e de parcelas em cada expressão:

(*a*) $E_L = 3 + 2 + 2 + 1 = 8$, $E_S = 4$.

(*b*) $E_L = 3 + 3 + 1 + 2 + 2 = 11$, $E_S = 5$

(*c*) $E_L = 3 + 4 + 3 = 10$, $E_S = 3$.

(*d*) Uma vez que E não é escrito como uma soma de produtos, E_L e E_S não estão definidos.

15.17 Considerando que E e F são somas de produtos Booleanas equivalentes, defina:

(*a*) E é mais simples do que F; (*b*) E é mínimo.

(*a*) E é mais simples do que F se $E_L < F_L$ e $E_S \leq F_S$ ou se $E_L \leq F_L$ e $E_S < F_S$.

(*b*) E é mínimo se não existe uma expressão de soma de produtos equivalente que seja mais simples do que E.

15.18 Encontre o consenso Q dos produtos fundamentais P_1 e P_2, onde:

(*a*) $P_1 = xy'z', P_2 = xyt$ (*c*) $P_1 = xy'z', P_2 = x'y'zt$

(*b*) $P_1 = xyz't, P_2 = xzt$ (*d*) $P_1 = xyz', P_2 = xz't$

O consenso Q de P_1 e P_2 existe se temos exatamente uma variável, digamos x_k, que seja complementada em P_1 ou em P_2 e não complementada no outro. Então Q é o produto (sem repetição) dos literais em P_1 e P_2, depois que x_k e x_k' tenham sido deletados.

(*a*) Delete y' e y e, em seguida, multiplique os literais de P_1 e P_2 (sem repetição) para obter $Q = xz't$.

(*b*) Deletando z' e z, temos $Q = xyt$

(*c*) Eles não possuem consenso, uma vez que, tanto x quanto z aparecem complementados em um dos produtos e não complementados no outro.

(*d*) Eles não possuem consenso, uma vez que nenhuma variável aparece complementada em um dos produtos e não complementada no outro.

15.19 Prove o Lema 15.10: Suponha que Q é o consenso de P_1 e P_2. Então, $P_1 + P_2 + Q = P_1 + P_2$.

Uma vez que os literais comutem, podemos assumir, sem perder a generalidade, que

$$P_1 = a_1 a_2 \cdots a_r t, \quad P_2 = b_1 b_2 \cdots b_s t', \quad Q = a_1 a_2 \cdots a_r b_1 b_2 \cdots b_s$$

Agora, $Q = Q(t + t') = Qt + Qt'$. Pois Qt contém P_1, $P_1 + Qt = P_1$, e porque Qt' contém P_2, $P_2 + Qt' = P_2$. Logo,

$$P_1 + P_2 + Q = P_1 + P_2 + Qt + Qt' = (P_1 + Qt) + (P_2 + Qt') = P_1 + P_2$$

15.20 Seja $E = xy' + xyz' + x'yz'$. Encontre: (*a*) os implicantes primos de E; (*b*) uma soma mínima para E.

(*a*) Aplique o Algoritmo 15.3 (método do consenso) como se segue:

$$\begin{aligned} E &= xy' + xyz' + x'yz' + xz' && \text{(consenso de } xy' \text{ e } xyz'\text{)} \\ &= xy' + x'yz' + xz' && \text{(}xyz' \text{ inclui } xz'\text{)} \\ &= xy' + x'yz' + xz' + yz' && \text{(consenso de } x'yz' \text{ e } xz'\text{)} \\ &= xy' + xz' + yz' && \text{(}x'yz' \text{ inclui } xz'\text{)} \end{aligned}$$

Nenhum passo no método do consenso pode ser aplicado agora. Logo, xy', xz' e yz' são os implicantes primos de E.

(*b*) Aplique o Algoritmo 15.4, escreva cada implicante primo de E na forma de soma de produtos completa para obter:

$$xy' = xy'(z + z') = xy'z + xy'z'$$
$$xz' = xz'(y + y') = xyz' + xy'z'$$
$$yz' = yz'(x + x') = xyz' + x'yz'$$

Apenas as parcelas xyz' e $xy'z'$ de xz' aparecem entre os outras parcelas, portanto, xz' pode ser eliminado, uma vez que é supérfluo. Logo, $E = xy' + yz'$ é uma soma mínima para E.

15.21 Seja $E = xy + y't + x'yz' + xy'zt'$. Encontre: (*a*) implicantes primos de E; (*b*) soma mínima para E.

(*a*) Aplique o Algoritmo 15.3 (método do consenso) como se segue:

$E = xy + y't + x'yz' + xy'zt' + xzt'$	(consenso de xy e $xy'zt'$)
$= xy + y't + x'yz' + xzt'$	($xy'zt'$ inclui xzt')
$= xy + y't + x'yz' + xzt' + yz'$	(consenso de xy e $x'yz'$)
$= xy + y't + xzt' + yz'$	($x'yz'$ inclui yz')
$= xy + y't + xzt' + yz' + xt$	(consenso de xy e $y't$)
$= xy + y't + xzt' + yz' + xt + xz$	(consenso de xzt' e xt)
$= xy + y't + yz' + xt + xz$	(xzt' inclui xz)
$= xy + y't + yz' + xt + xz + z't$	(consenso de $y't$ e yz')

Nenhum passo no método do consenso pode ser aplicado agora. Logo, os implicantes primos de E são xy, $y't$, yz', xt, xz e $z't$.

(*b*) Aplique o Algoritmo 15.4, isto é, escreva cada implicante primo na forma de soma de produtos completa e, então, delete os supérfluos, um por um, isto é, aqueles cujas parcelas aparecem entre as outras parcelas. Isso, finalmente, implica

$$E = y't + xz + yz'$$

como uma soma mínima para E.

Portões lógicos

15.22 Expresse a saída Y de uma expressão Booleana nas entradas A, B e C para o circuito lógico em.

(*a*) Fig. 15-26(*a*); (*b*) Fig. 15-36(*b*).

(*a*) As entradas para o primeiro portão AND são A e B' e para o segundo portão AND são B' e C. Logo, $Y = AB' + B'C$

(*b*) As entradas para o primeiro portão AND são A e B' e para o segundo portão AND são A' e C. Logo, $Y = AB' + A'C$

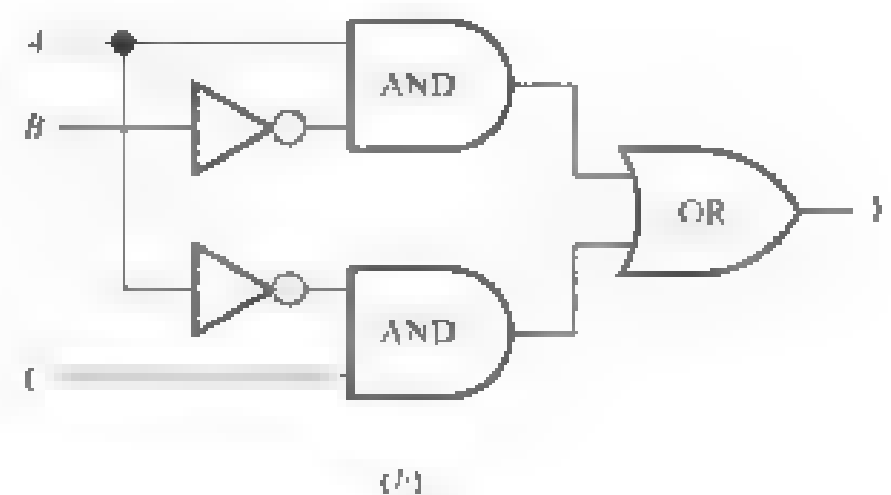
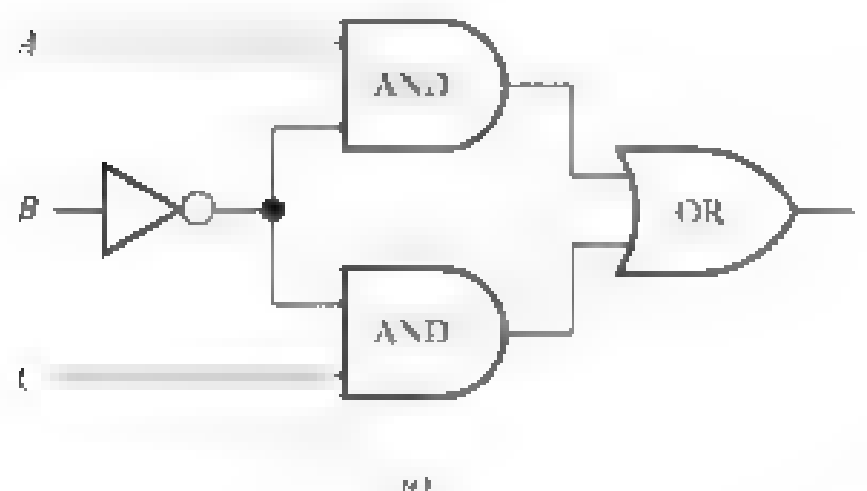



Figura 15-26

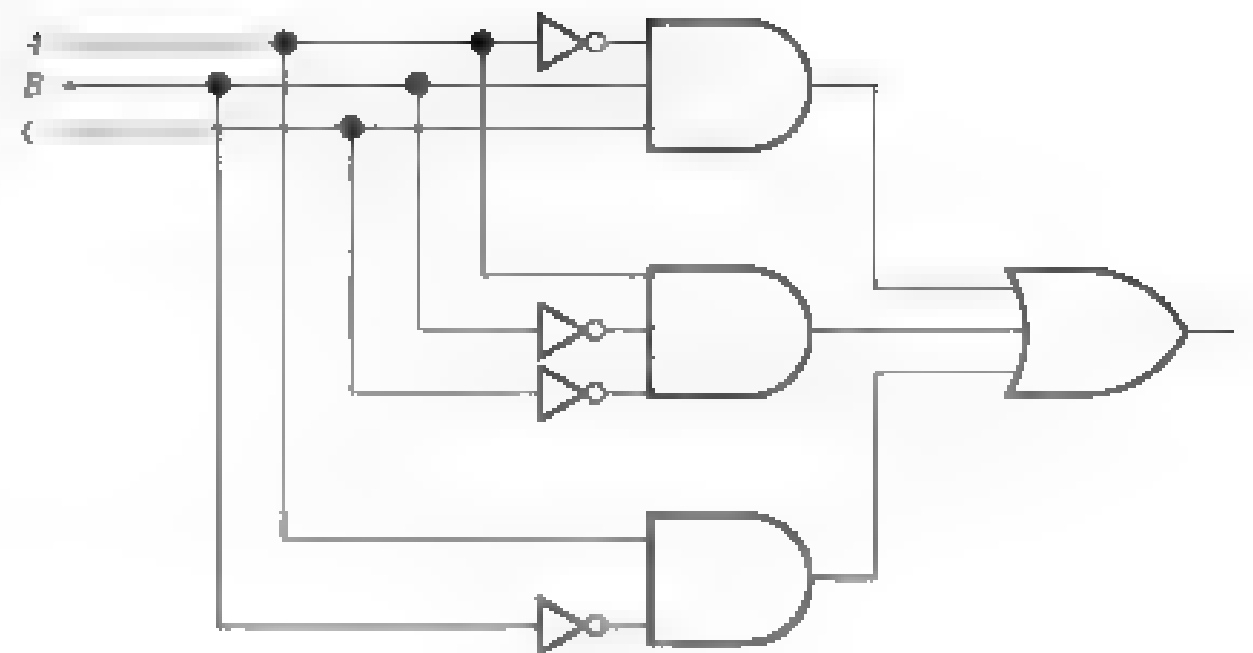



Figura 15-27

15.23 Expresse a saída Y como uma expressão Booleana nas entradas A, B e C para o circuito lógico na Fig. 15-27.

A saída do primeiro portão AND é $A'BC$, do segundo portão AND é $A'B'C'$ e do último portão AND é AB'

Logo,

$$Y = A'BC + AB'C' + AB'$$

15.24 Expresse a saída Y como uma expressão Booleana nas entradas A, B e C para o circuito lógico em:

(a) Fig. 15-28(a); (b) Fig. 15-28(b).

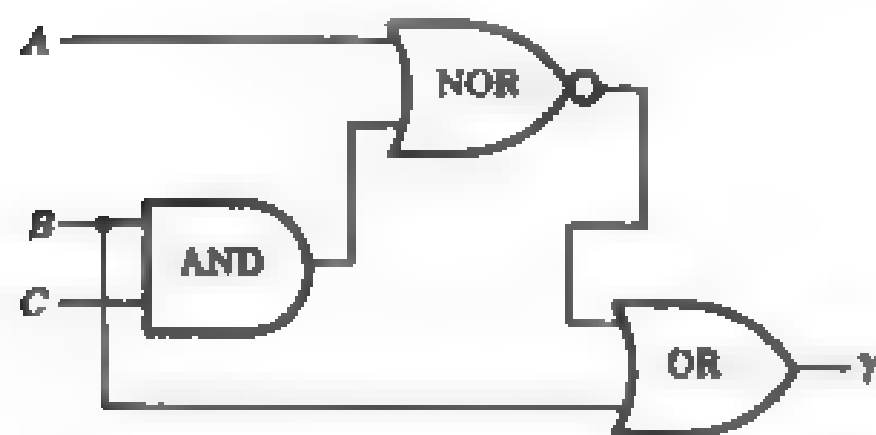
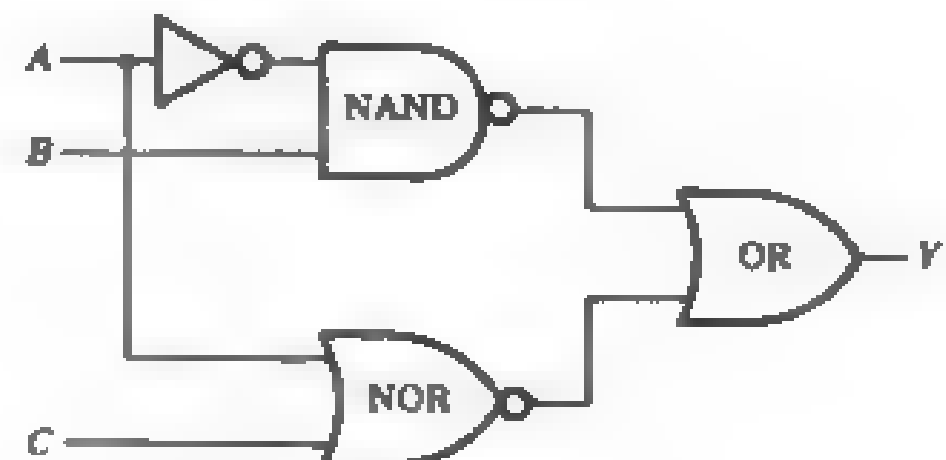



Figura 15-28

(a) A saída do portão AND é BC, portanto, as entradas do portão NOR são A e BC. Logo, $(A + BC)'$ é a saída do portão NOR. Portanto, as entradas do portão OR são $(A + BC)'$ e B; então, $Y = (A + BC)' + B$

(b) A saída do portão NAND é $(A'B)'$ e a saída do portão NOR é $(A + C)'$. Logo, $Y = (A'B)' + (A + C)'$

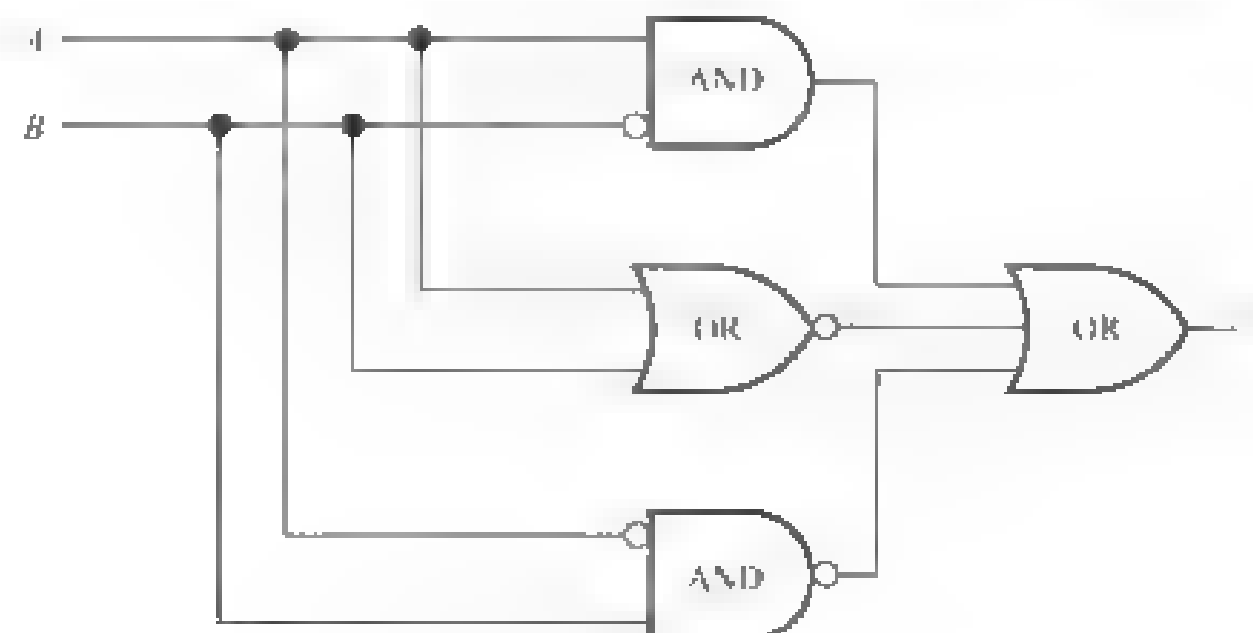



Figura 15-29

15.25 Expresse a saída Y como uma expressão Booleana nas entradas A e B para o circuito lógico na Fig. 15-29.

Aqui, um pequeno círculo no circuito significa um complemento. Logo, as saídas dos três portões à esquerda são AB', $(A + B)'$ e $(A'B)'$. Logo,

$$Y = AB' + (A + B)' + (A'B)'$$

15.26 Esboce o circuito lógico L com entradas A, B e C e saída Y que corresponde a cada uma das expressões Booleanas:

(a) $Y = ABC + A'C' + B'C'$; (b) $Y = AB'C + ABC' + AB'C'$.

Essas são expressões de soma de produtos. Logo, L será um circuito AND-OR que possui um portão AND para cada produto e um portão OR para a soma. Os circuitos pedidos aparecem na Fig. 15-30(a) e (b).

(a) $Y = ABC + A'C' + B'C'$ (b) $Y = AB'C + ABC' + AB'C'$

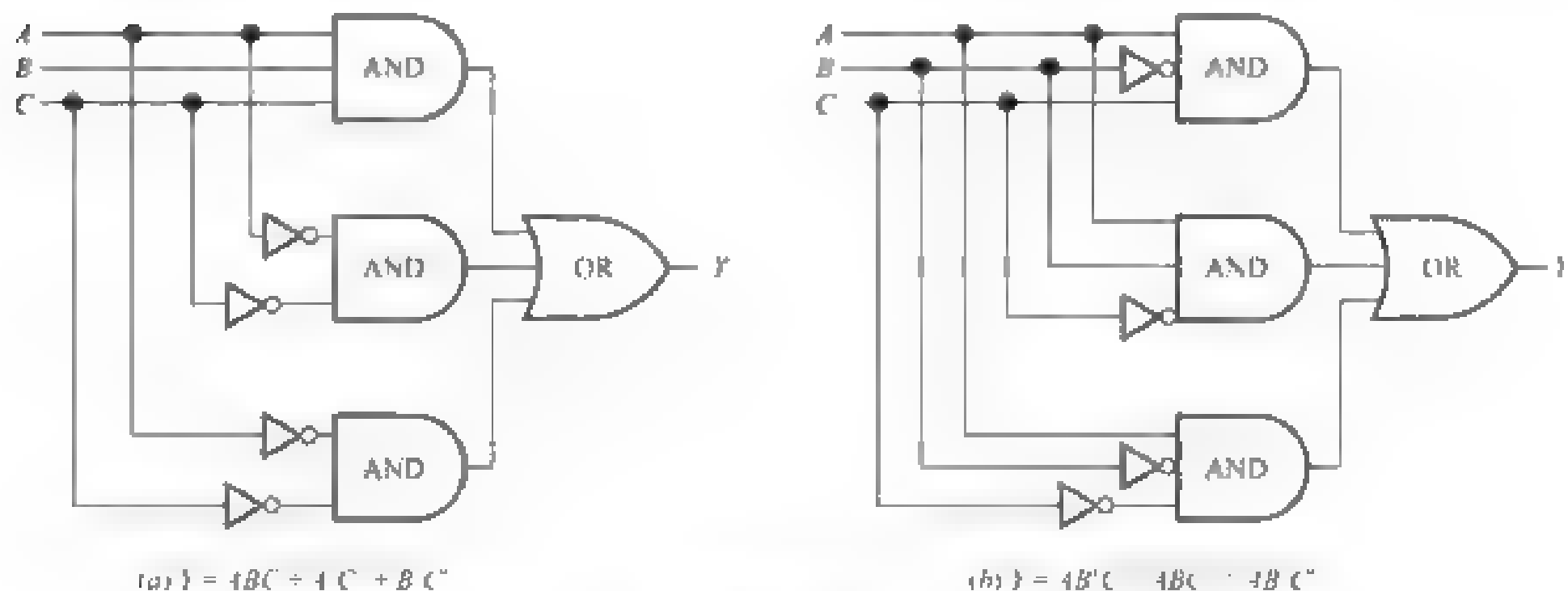



Figura 15-30

Tabelas verdade

15.27 Encontre a sequência de saída Y para um portão AND com entradas A, B e C (ou, de forma equivalente, para $Y = ABC$), onde:

(a) $A = 111001$; $B = 100101$; $C = 110011$.

(b) $A = 11111100$; $B = 10101010$; $C = 00111100$.

(c) $A = 00111111$; $B = 11111100$; $C = 11000011$.

A saída $Y = 1$ para um portão AND se, e somente se, existem 1's em todas as posições das sequências de entrada. Logo,

(a) Apenas a primeira e a última posição possuem 1's em todas as três sequências. Logo, $Y = 100001$

(b) Apenas a terceira e a quinta posição (lendo da esquerda para a direita) possuem 1's em todas as três sequências. Logo, $Y = 00101000$

(c) Nenhuma posição possui 1's em todas as três sequências. Logo, $Y = 00000000$.

15.28 Encontre a sequência de saída para um portão OR com entradas A, B e C (ou, de forma equivalente, para $Y = A + B + C$), onde:

(a) $A = 100001$; $B = 100100$; $C = 110000$.

(b) $A = 11000000$; $B = 10101010$; $C = 00000011$.

(c) $A = 00111111$; $B = 11111100$; $C = 11000011$.

A saída $Y = 0$ para um portão OR se, e somente se, existem 0's em todas as posições das sequências de entrada. Logo:

(a) Apenas a terceira e a quinta posição possuem 0's em todas as três sequências. Logo, $Y = 110101$

(*b*) Apenas a quarta e a sexta posição (lendo da esquerda para a direita) possuem 0's em todas as três sequências. Logo, $Y = 11101011$

(*c*) Nenhuma posição possui 0's em todas as três sequências. Logo, $Y = 11111111$

15.29 Encontre a sequência Y de saída para um portão NOT com entrada A ou, de forma equivalente, para $Y = A'$, onde.

(*a*) $A = 00111111$; (*b*) $A = 11111100$; (*c*) $A = 11000011$

O portão NOT muda 0 para 1 e 1 para 0. Logo:

(*a*) $A' = 11000000$; (*b*) $A' = 00000011$; (*c*) $A' = 00111100$.

15.30 Considere um circuito lógico com $n = 5$ entradas A, B, C, D e E ou, de forma equivalente, considere uma expressão Booleana E com cinco variáveis x_1, x_2, x_3, x_4 e x_5.

(*a*) Encontre as sequências especiais para as variáveis (entradas).

(*b*) Quantas maneiras diferentes existem de associarmos um bit (0 ou 1) para cada uma das $n = 5$ variáveis?

(*c*) Qual é a principal propriedade das sequências especiais?

(*a*) Todas as sequências possuem comprimento $2^n = 2^5 = 32$. Elas virão consistir de blocos alternados de 0's e 1's em que, os comprimentos dos blocos são $2^{n-1} = 2^4 = 16$ para x_1, $2^{n-2} = 2^3 = 8$ para x_2, ..., $2^{n-5} = 2^0 = 1$ para x_5. Logo:

$$x_1 = 00000000000000001111111111111111$$
$$x_2 = 00000000111111110000000011111111$$
$$x_3 = 00001111000011110000111100001111$$
$$x_4 = 00110011001100110011001100110011$$
$$x_5 = 01010101010101010101010101010101$$

(*b*) Existem duas maneiras, 0 ou 1, de associar um bit para cada variável e, portanto, existem $2^n = 2^5 = 32$ maneiras de associar um bit a cada uma das $n = 5$ variáveis

(*c*) As 32 posições nas sequências especiais dão todas as 32 possíveis combinações de bits para as cinco variáveis

15.31 Encontre a tabela verdade $T = T(E)$ para a expressão Booleana $E = E(x, y, z)$ onde:

(*a*) $E = xz + x'y$, (*b*) $E = xy'z + xy + z'$

As sequências especiais para as variáveis x, y e z e seus complementos são listados a seguir:

$$x = 00001111, \quad y = 00110011, \quad z = 01010101$$
$$x' = 11110000, \quad y' = 11001100, \quad z' = 10101010$$

(*a*) Aqui $xz = 00000101$ e $x'y = 00110000$. Então $E = xz + x'y = 00110101$. Logo,

$$T(00001111, 00110011, 01010101) = 00110101$$

ou, simplesmente, $T(E) = 00110101$, onde assumimos que a entrada consiste nas sequências especiais.

(*b*) Aqui, $xy'z = 00000100$, $xy = 00000011$ e $z' = 01010101$. Então $E = xy'z + xy + z' = 01010111$. Logo,

$$T(00001111, 00110011, 01010101) = 01010111$$

15.32 Encontre a tabela verdade $T = T(E)$ para a expressão Booleana $E = E(x, y, z)$ onde:

(*a*) $E = xyz' + x'yz$; (*b*) $E = xyz + xy'z + x'y'z$.

Aqui, E é uma expressão de soma de produtos completa, que é a soma de mintermos. O Exemplo 15.13 nos dá as tabelas verdade para os mintermos (usando as sequências especiais). Cada mintermo contém um único 1 em sua tabela verdade; logo, a tabela verdade de E terá 1's nos mintermos em E. Logo:

(*a*) $T(E) = 00001010$; (*b*) $T(E) = 01000101$

15.33 Encontre a tabela verdade $T = T(E)$ para a expressão Booleana

$$E = E(x, y, z) = (x' y)' yz' + x'(yz + z')$$

Primeiro, expresse E como uma soma de produtos.

$$E = (x + y')yz' + x'yz + x'z' = xyz' + y'yz' + x'yz + x'z'$$
$$= xyz' + x'yz + x'z'$$

Agora, expresse E como uma soma de produtos completa.

$$E = xyz' + x'yz + x'z'(y + y')$$
$$= xyz' + x'yz + x'yz' + x'y'z'$$

Como no Problema 15.32, use as tabelas verdade para os mintermos que aparecem no Exemplo 15.13, para obter $T(E) = 10101010$.

15.34 Encontre a expressão Booleana $E = E(x, y, z)$ que corresponde à tabela verdade:

(*a*) $T(E) = 01001001$; (*b*) $T(E) = 00010001$.

Cada 1 em $T(E)$ corresponde ao mintermo com o 1 na mesma posição (usando as tabelas verdade para os mintermos que aparecem no Exemplo 15.13). Por exemplo, o 1 na segunda posição corresponde a $x'y'z$ cuja tabela verdade possui um único 1 na segunda posição. Então, E é a soma desses mintermos. Logo:

(*a*) $E = x'y'z + x'yz + xyz'$; (*b*) $E = xy'z' + xyz$

(Novamente, assumimos que a entrada consiste em sequências especiais.)

Mapas de Karnaugh

15.35 Encontre o produto fundamental P representado por cada um dos retângulos básicos no mapa de Karnaugh da Fig. 15-31.

Em cada caso, encontre os literais que aparecem em todos os quadrados do retângulo básico, então, P é o produto desses literais.

(*a*) x' e z' aparecem em ambos os quadrados; logo, $P = x'z'$.

(*b*) x e z aparecem em ambos os quadrados, logo, $P = xz$.

(*c*) Apenas z aparece em todos os quatro quadrados; logo, $P = z$.

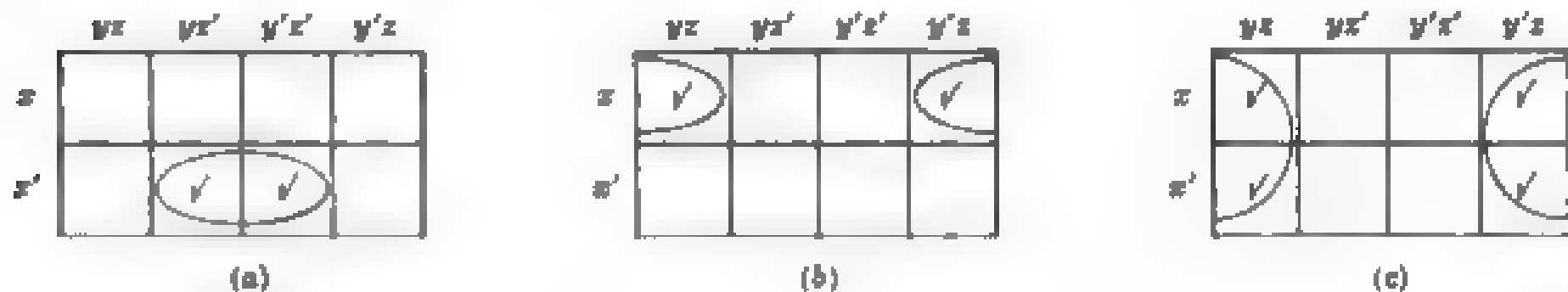



Figura 15-31

15.36 Seja R um retângulo básico em um mapa de Karnaugh para quatro variáveis x, y, z e t. Encontre o número de literais no produto fundamental P que corresponde a R em termos do número de quadrados de R.

P terá um, dois, três ou quatro literais, considerando que R possui oito, quatro, dois ou um quadrado.

15.37 Encontre o produto fundamental P representado por cada retângulo básico R no mapa de Karnaugh na Fig. 15-32.

Em cada caso, encontre os literais que aparecem em todos os quadrados do retângulo básico, então, P é o produto desses literais. (O Problema 15.36 indica o número de literais em P.)

(*a*) Existem dois quadrados em R, então P possui três literais. Especificamente, x', y' e t' aparece em ambos os quadrados; logo, $P = x'y't$.

(*b*) Existem quatro quadrados em R, então P possui dois literais. Especificamente, y' e t aparecem em todos os quatro quadrados; logo, $P = y't$.

(*c*) Existem oito quadrados em R, então P possui apenas um literal. Especificamente, apenas y aparece em todos os oito quadrados; logo, $P = y$.

(a)

(b)

(c)

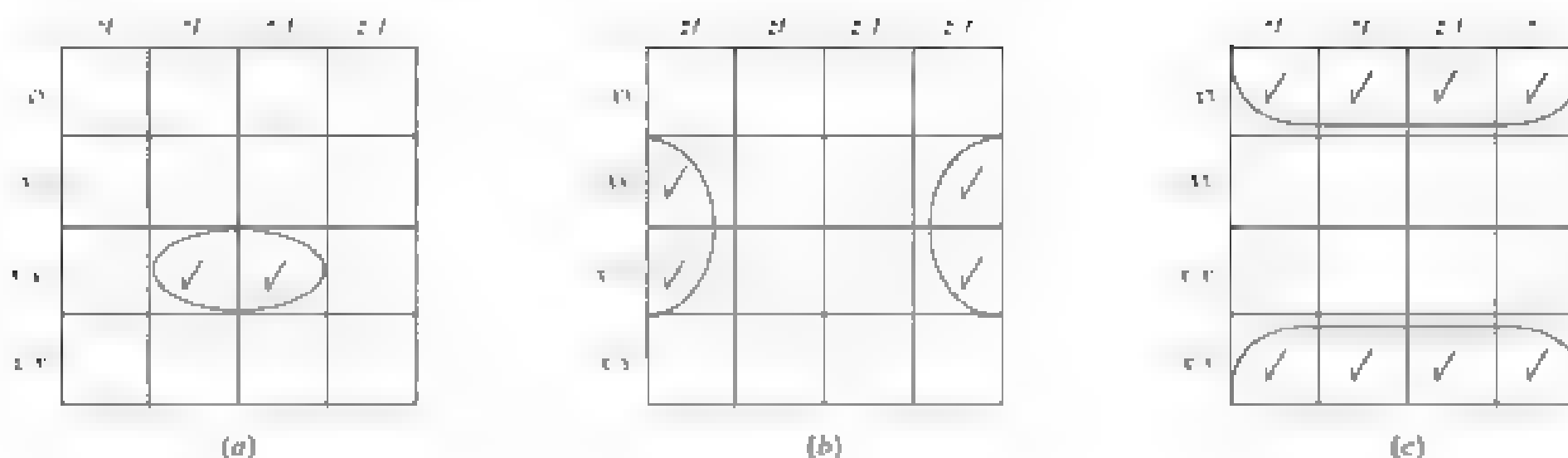



Figura 15-32

15.38 Seja E uma expressão Booleana apresentada no mapa de Karnaugh na Fig. 15-33

(a) Escreva E em sua forma de soma de produtos completa. (b) Encontre uma forma mínima para E.

(a) Liste os sete produtos fundamentais assinalados para obter

$$E = xyz't' + xyz't + xy'zt + xy'zt' + x'y'zt + x'y'zt' + x'yz't'$$

(b) Os dois retângulos básicos máximos de área dois por dois representam $y'z$, uma vez que apenas y' e z aparecem em todos os quatro quadrados. O par horizontal de quadrados adjacentes representam xyz' e os quadrados adjacentes que sobrepõe as arestas superior e inferior representam $yz't'$. Todos os três retângulos são necessários para uma cobertura mínima,

$$E = y'z + xyz' + yz't'$$

é a soma mínima para E.

15.39 Considere as expressões Booleanas E_1 e E_2 em variáveis x, y, z e t que são dadas pelos mapas de Karnaugh na Fig. 15-34. Encontre uma soma mínima para (a) E_1; (b) E_2.

(a) Apenas y' aparece em todos os oito quadrados do retângulo básico máximo de área dois por dois e o par escolhido de quadrados adjacentes representam xzt'. Já que ambos os retângulos são necessários para uma cobertura mínima,

$$E_1 = y' + xzt'$$

é a soma mínima para E_1.

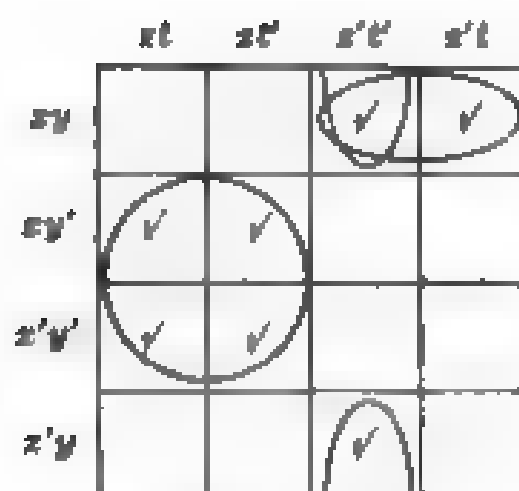



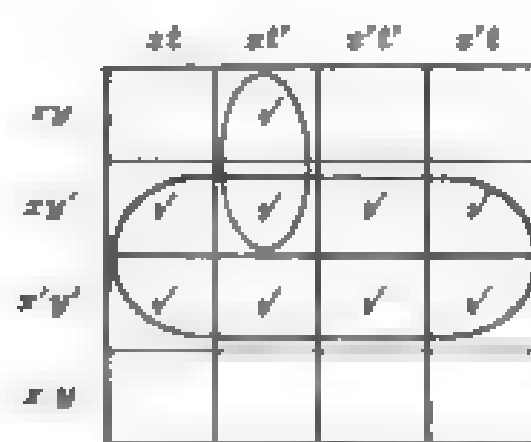
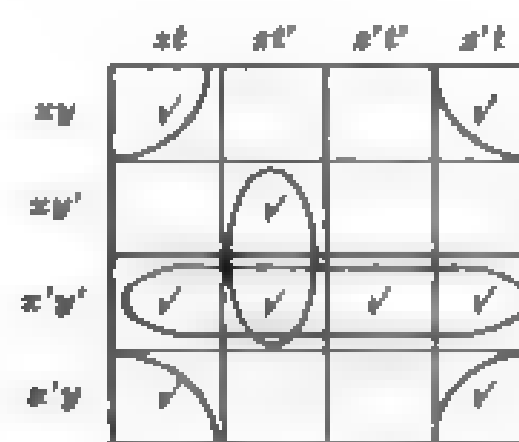
Figura 15-33

(a) E_1

(b) E_2

Figura 15-34

(b) Os quatro quadrados nos cantos formam um retângulo básico máximo de área dois por dois que representa yt, uma vez que apenas y e t aparecem em todos os quatro quadrados. O retângulo básico máximo de área quatro por um representa $x'y'$ e os dois quadrados adjacentes representam $y'zt'$. Todos os três retângulos são necessários para uma cobertura mínima,

$$E_2 = yt + x'y' + y'zt'$$

é a soma mínima para E_2.

15.40 Considere as expressões Booleanas E_1 e E_2 nas variáveis x, y, z e t que são dadas pelos mapas de Karnaugh na Fig. 15-35. Encontre uma soma mínima para (*a*) E_1; (*b*) E_2.

(*a*) Existem cinco implicantes primos, designados pelas quatro voltas e pelo círculo sombreado. Contudo, o círculo sombreado não é necessário para cobrir todos os quadrados, é preciso apenas as quatro voltas. Portanto, as quatro voltas dão a soma mínima para E_1; ou seja,

$$E_1 = xzt' + xy'z' + x'y'z + x'z't'$$

(*b*) Existem cinco implicantes primos, designados pelas cinco voltas, das quais duas são sombreadas. Apenas uma das duas voltas sombreadas é necessária para cobrir o quadrado $x'y'z't'$. Logo, existem duas somas mínimas para E_2, como se segue.

$$E_2 = x'y + yt + xy't' + y'z't' = x'y + yt + xy't' + x'z't'$$

(a) E_1

(b) E_2

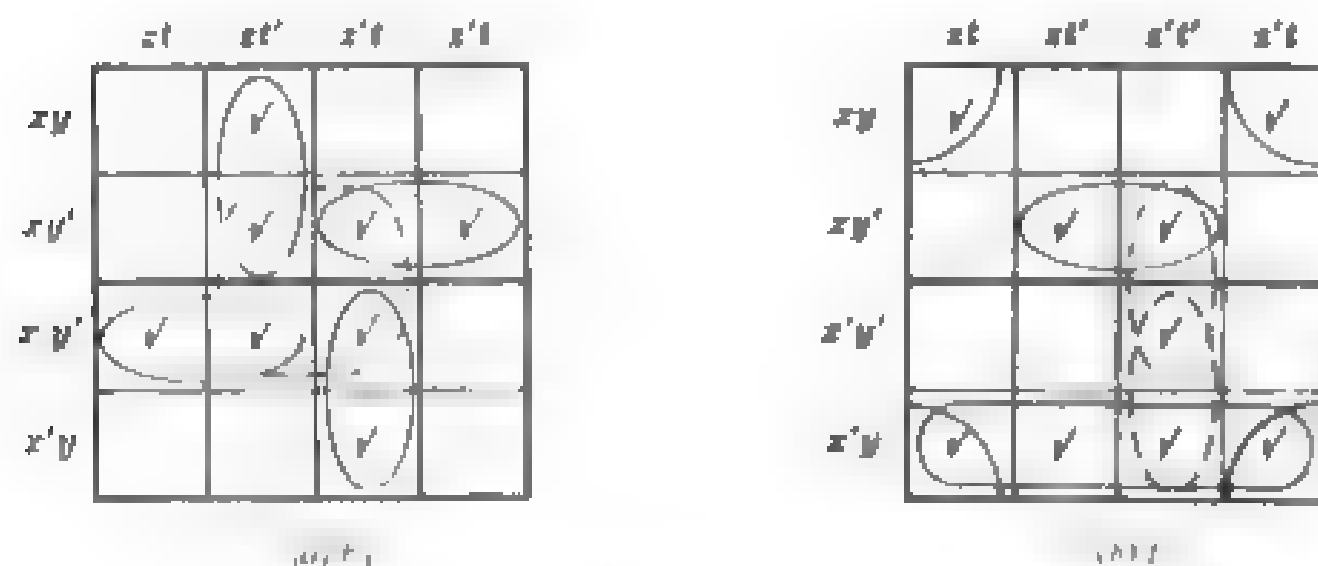



Figura 15-35

15.41 Use um mapa de Karnaugh para encontrar uma soma mínima para:

(*a*) $E_1 = x'yz + x'yz't + y'zt' + xyzt' + xy'z't'$.

(*b*) $E_2 = y't' + y'z't + x'y'zt + yzt'$

(*a*) Marque os dois quadrados que correspondem a $x'yz$ e $y'zt'$, assim como o quadrado que corresponde a $x'yz't$, $xyzt'$ e $xy'z't'$. Isso nos dá o mapa de Karnaugh da Fig. 15-36(*a*). Uma cobertura mínima consiste nas três curvas designadas. Logo, uma soma mínima para E_1 é a que se segue:

$$E_1 = zt' + xy't' + x'yt$$

(*b*) Marque os quatro quadrados correspondentes a zt' os dois quadrados que correspondem a $y'z't$ e yzt', como também o quadrado que corresponde a $x'y'zt$. Isso nos dá o mapa de Karnaugh na Fig. 15-36(*b*). Uma cobertura mínima consiste nos três retângulos básicos máximos designados. Logo, uma soma mínima para E_2 é a que se segue

$$E_2 = zt' + xy't' + x'yt$$

(a) E_1

(b) E_2

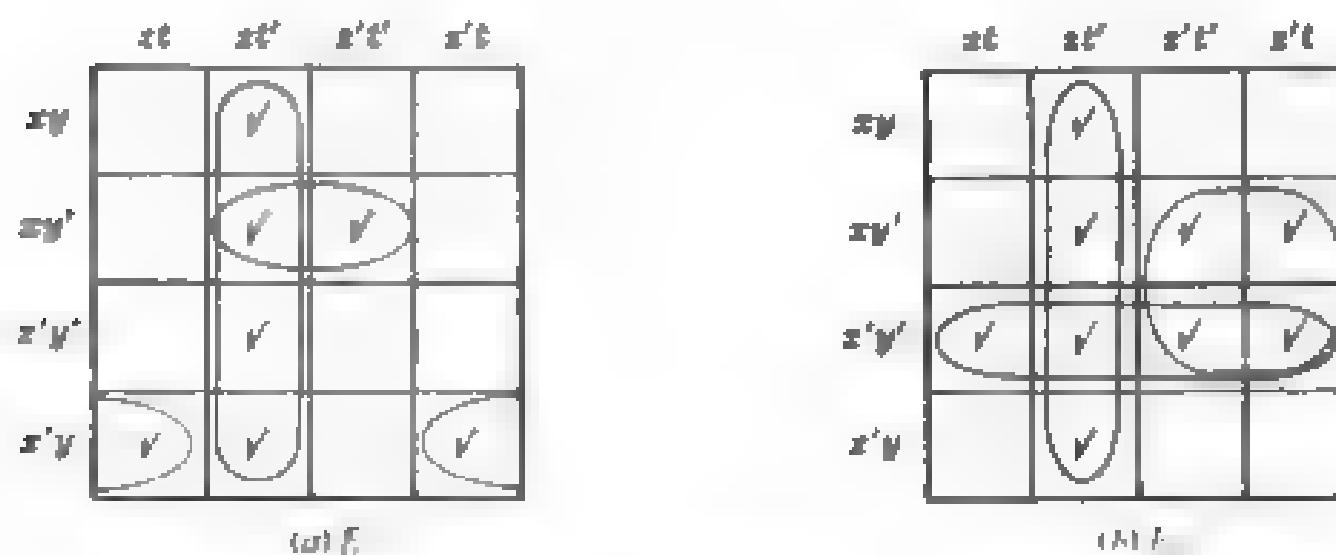



Figura 15-36

15.42 Encontre uma forma mínima de soma de produtos para a expressão Booleana E com as tabelas verdade a seguir:

(*a*) $T(00001111, 00110011, 01010101) = 10100110$.

(*b*) $T(00001111, 00110011, 01010101) = 00101111$.

(*a*) A partir da tabela verdade T apresentada (e das tabelas verdade no Exemplo 15.13 para os mintermos nas variáveis x, y e z), podemos ler a forma de soma de produtos completa para E:

$$E = x'y'z' + x'yz' + xy'z + xyz'$$

Seu mapa de Karnaugh aparece na Fig. 15-37(*a*). Existem três implicantes primos, como indicado no mapa pelas três curvas, que formam uma cobertura mínima de E. Logo, uma forma mínima para E é a que se segue:

$$E = yz' + x'z' + xy'z$$

(*b*) A partir da tabela verdade apresentada, podemos ler a forma de soma de produtos completa para E:

$$E = x'yz' + x'yz + xy'z + xyz' + xyz$$

Seu mapa de Karnaugh aparece na Fig. 15-37(*b*). Existem dois implicantes primos, como indicado pelas duas voltas, que formam uma cobertura mínima de E. Logo, uma forma mínima para E é a que se segue:

$$E = xz + y$$

(*a*)

(*b*)

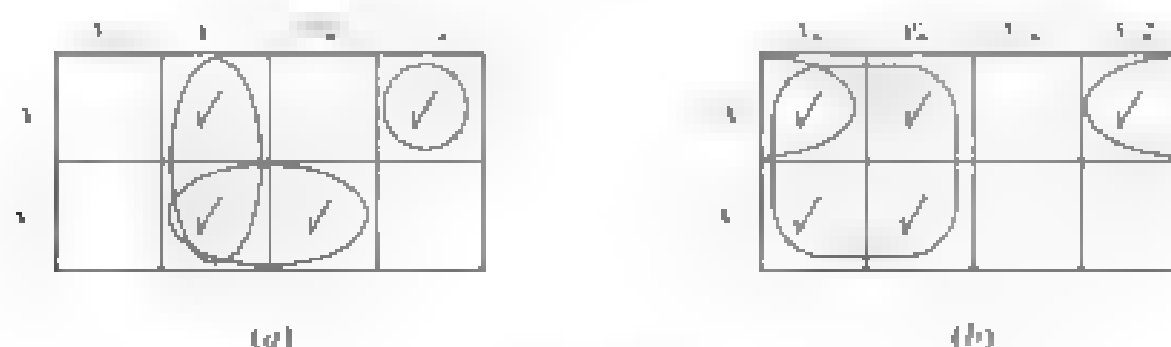



Figura 15-37

Problemas Complementares

Álgebras Booleanas

15.43 Escreva a dual de cada uma das expressões Booleanas a seguir:

(a) $a(a' + b) = ab$ (b) $(a + 1)(a + 0) = a$ (c) $(a + b)(b + c) = ac + b$

15.44 Considere os reticulados $\mathbf{D}_m$ de divisores de m (onde $m > 1$).

(a) Mostre que $\mathbf{D}_m$ é uma álgebra Booleana se, e somente se, m é *livre de quadrados*, isto é, se m é um produto de primos distintos.

(b) Se $\mathbf{D}_m$ é uma álgebra Booleana, mostre que os átomos são os divisores primos distintos de m.

15.45 Considere os reticulados a seguir: (a) $\mathbf{D}_{20}$, (b) $\mathbf{D}_{55}$, (c) $\mathbf{D}_{99}$, (d) $\mathbf{D}_{130}$. Quais deles são álgebras Booleanas, e quais são seus átomos?

15.46 Considere a álgebra Booleana $\mathbf{D}_{110}$.

(a) Liste seus elementos e esboce seu diagrama.

(b) Encontre todas as suas subálgebras.

(c) Encontre o número de subreticulados com quatro elementos.

(d) Encontre o conjunto A de átomos de $\mathbf{D}_{110}$.

(e) Apresente o mapeamento isomórfico $f: \mathbf{D}_{110} \to P(A)$, como definido no Teorema 15.6.

15.47 Seja B uma álgebra Booleana. Mostre que:

(a) Para qualquer x em B, $0 \leq x \leq 1$. (b) $a < b$ se, e somente se, $b' < a'$.

15.48 Um elemento x em uma álgebra Booleana é chamado de *maxtermo* se a identidade 1 é seu único sucessor. Encontre os maxtermos na álgebra Booleana $\mathbf{D}_{210}$ apresentada na Fig. 15-25.

15.49 Seja B uma álgebra Booleana.

(a) Mostre que os complementares dos átomos de B são maxtermos.

(b) Mostre que qualquer elemento x em B pode ser expresso unicamente como um produto de maxtermos

15.50 Seja B uma álgebra Booleana com 16 elementos, e considere S como sendo uma subálgebra de B com oito elementos. Mostre que dois dos átomos de S devem ser átomos de B.

15.51 Seja $B = (B, +, *, ', 0, 1)$ a álgebra Booleana. Defina uma operação Δ em B (chamada de *diferença simétrica*) por meio de

$$x \Delta y = (x * y') + (x' * y)$$

Prove que $R = (B, \Delta, *)$ é um anel Booleano comutativo. (Veja a Seção B.6 e o Problema B.72.)

15.52 Seja $R = (R, \oplus, \cdot)$ um anel Booleano com identidade $1 \neq 0$. Defina

$$x' = 1 \oplus x, \quad x + y = x \oplus y \oplus x \cdot y, \quad x * y = x \cdot y$$

Prove que $B = (R, +, *, ', 0, 1)$ é uma álgebra Booleana.

Expressões Booleanas, implicantes primos

15.53 Reduza os produtos Booleanos a seguir para 0 ou para um produto fundamental

(a) $xy'zxy'$; (b) $xyz'sy'ts$; (c) $xy'xz'ty'$; (d) $xyz'ty't$.

15.54 Escreva cada expressão Booleana $E(x, y, z)$ como uma soma de produtos e, em seguida, na sua forma de soma de produtos completa:

(a) $E = x(xy' + x'y + y'z)$; (b) $E = (x + y'z)(y + z')$; (c) $E = (x' + y)' + y'z$

15.55 Escreva cada expressão Booleana $E(x, y, z)$ como uma soma de produtos e, em seguida, na sua forma de soma de produtos completa.

(a) $E = (x'y)'(x' + xyz')$; (b) $E = (x + y)'(xy')'$; (c) $E = y(x + yz)'$

15.56 Encontre o consenso Q dos produtos fundamentais P_1 e P_2 onde:

(a) $P_1 = xy'z$, $P_2 = xyt$; (c) $P_1 = xy'zt$, $P_2 = xyz'$;

(b) $P_1 = xyz't'$, $P_2 = xzt'$; (d) $P_1 = xy't$, $P_2 = xzt$.

15.57 Para qualquer expressão Booleana de soma de produtos E, assumimos que E_L denota o número de literais em E (contando multiplicidade) e E_S denota o número de parcelas em E. Encontre E_L e E_S para cada um dos seguintes.

(a) $E = xyz't + x'yt + xy'zt$; (b) $E = xyzt + xt' + x'y't + yt$

15.58 Aplique o método do consenso (Algoritmo 15.3) para encontrar os implicantes primos de cada expressão Booleana:

(a) $E_1 = xy'z' + x'y + x'y'z' + x'yz$;

(b) $E_2 = xy' + x'z't + xyzt' + x'y'zt'$;

(c) $E_3 = xyzt + xyz't' + xz't' + x'y'z' + x'yz't$

15.59 Encontre a forma mínima de soma de produtos para cada uma das expressões Booleanas do Problema 15.58.

Portões lógicos, tabelas verdade

15.60 Expresse a saída Y como uma expressão Booleana nas entradas A, B e C para o circuito lógico em:

(a) Fig. 15-38(a); (b) Fig. 15-38(b).

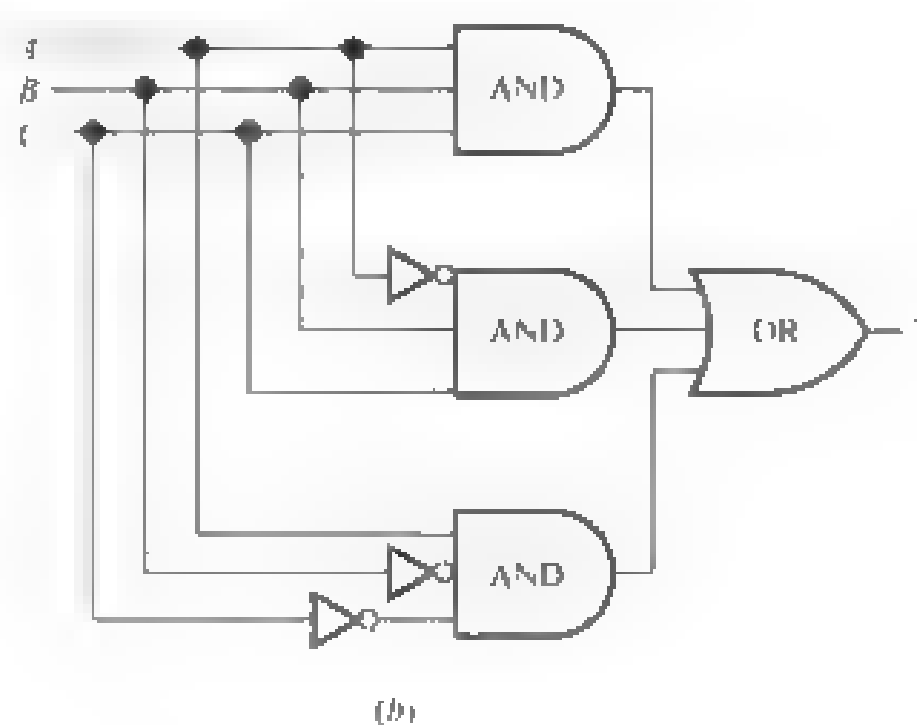
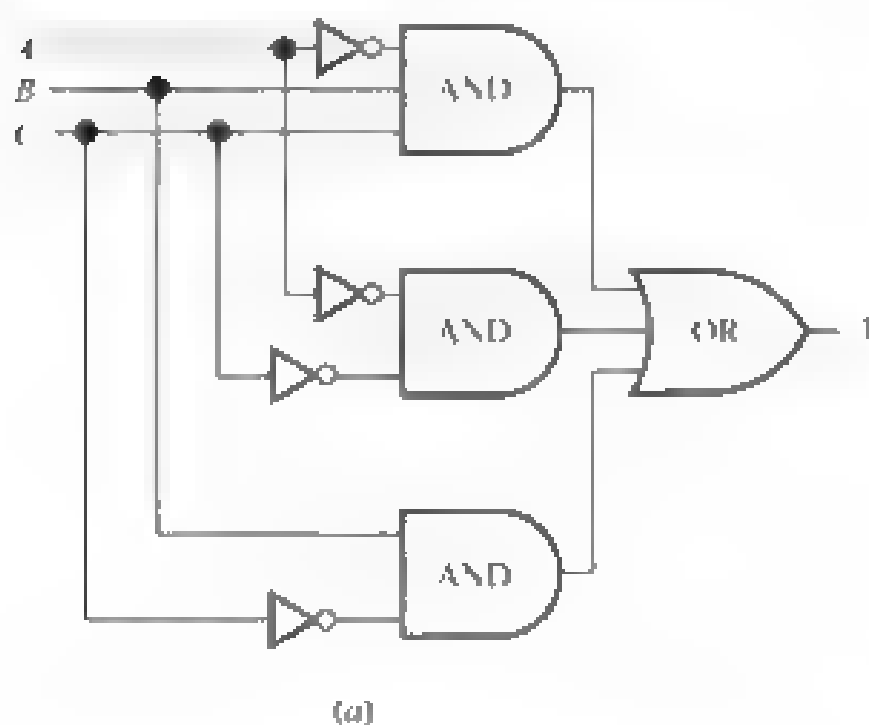



Figura 15-38

15.61 Escreva a saída Y como uma expressão Booleana nas entradas A, B e C para o circuito lógico em:

(a) Fig. 15-39(a); (b) Fig. 15-39(b).

15.62 Esboce o circuito lógico L com entradas A, B e C e saída Y que corresponda a cada uma das expressões Booleanas.

(a) $Y = AB'C + AC' + A'C$; (b) $Y = A'BC + A\,BC' + ABC'$.

15.63 Encontre a sequência de saída Y para um portão AND com entradas A, B e C (ou, de forma equivalente, para $Y = ABC$) onde:

(a) $A = 110001$, $B = 101101$; $C = 110011$

(b) $A = 01111100$; $B = 10111010$; $C = 00111100$.

(c) $A = 00111110$; $B = 01111100$; $C = 11110011$.

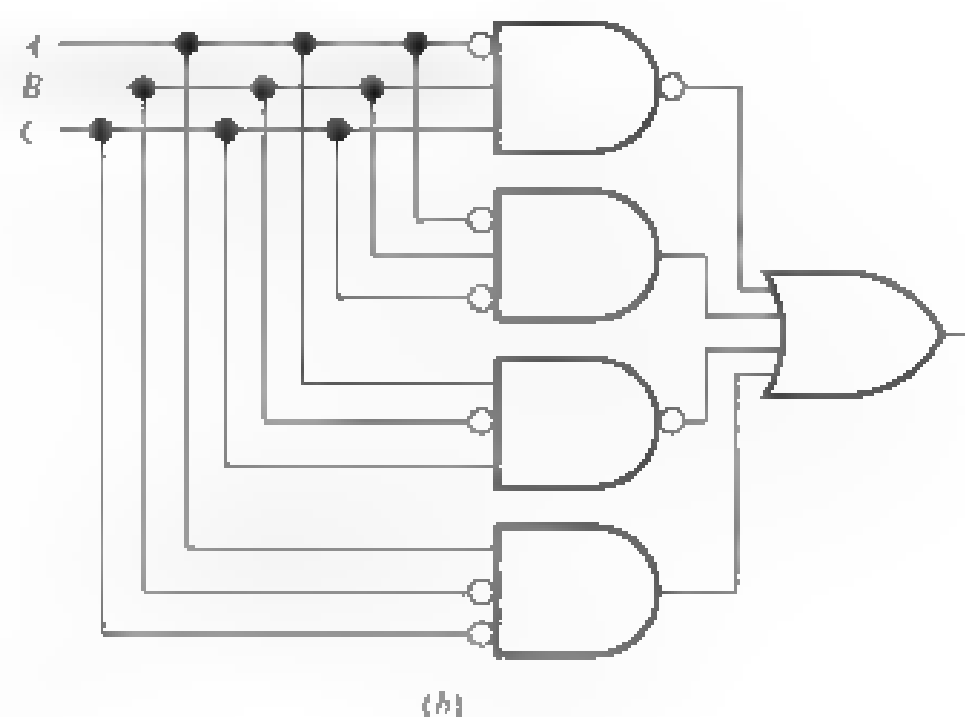
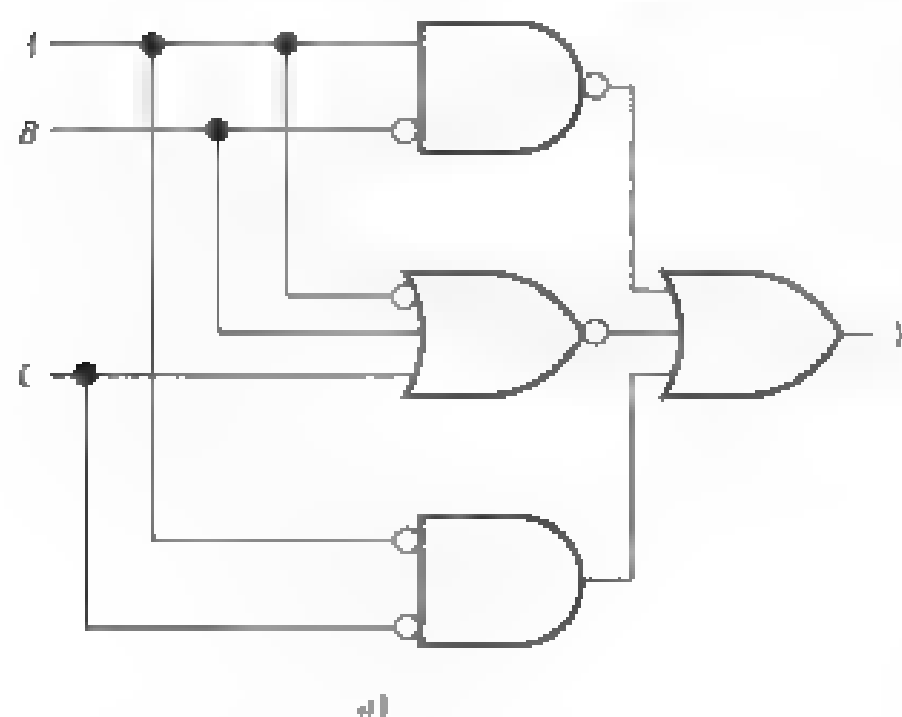



Figura 15-39

15.64 Encontre a sequência de saída Y para um portão OR com entradas A, B e C (ou, de forma equivalente, para $Y = A + B + C$) onde:

(a) $A = 100011$; $B = 100101$; $C = 1000001$.

(b) $A = 10000001$; $B = 00100100$; $C = 00000011$.

(c) $A = 00111100$, $B = 11110000$; $C = 10000001$

15.65 Encontre a sequência de saída Y para um portão NOT com entrada A ou, de forma equivalente, para $Y = A'$, onde:

(a) $A = 11100111$; (b) $A = 10001000$; (c) $A = 11111000$.

15.66 Considere um circuito lógico L com $n = 6$ entradas A, B, C, D, E e F ou, de forma equivalente, considere uma expressão Booleana E com seis variáveis $x_1, x_2, x_3, x_4, x_5, x_6$.

(a) Quantas maneiras diferentes existem para associarmos um bit (0 ou 1) a cada uma das $n = 6$ variáveis?

(b) Encontre as três primeiras sequências especiais para as variáveis (entradas).

15.67 Encontre a tabela verdade $T = T(E)$ para a expressão Booleana $E = E(x, y, z)$ onde:

(a) $E = xy + x'z$; (b) $E = xyz' + y + xy'$.

15.68 Encontre a tabela verdade $T = T(E)$ para a expressão Booleana $E = E(x, y, z)$ onde:

(a) $E = x'yz' + x'y'z$; (b) $E = xyz' + xy'z' + x'y'z'$.

15.69 Encontre a expressão Booleana $E = E(x, y, z)$ correspondente às tabelas verdade:

(a) $T(E) = 10001010$; (b) $T(E) = 00010001$; (c) $T(E) = 00110000$.

15.70 Encontre todas as somas mínimas possíveis para cada expressão Booleana E apresentada pelos mapas de Karnaugh na Fig. 15-40.

(a)

(b)

(c)

Figura 15-40

15.71 Encontre todas as somas mínimas possíveis para cada expressão Booleana E apresentada pelos mapas de Karnaugh na Fig. 15-41.

(a)

(b)

(c)

Figura 15-41

15.72 Use um mapa de Karnaugh para encontrar uma soma mínima para a expressão Booleana.

(a) $E = xy + x'y + x'y'$; (b) $E = x + x'yz + xy'z'$.

15.73 Encontre a soma mínima para cada expressão Booleana:

(a) $E = y'z + y'z't' + z't$; (b) $E = y'zt + xzt' + xy'z'$.

15.74 Use mapas de Karnaugh para redesenhar cada circuito na Fig. 15-42 de forma que eles se tornem circuitos mínimos AND-OR.

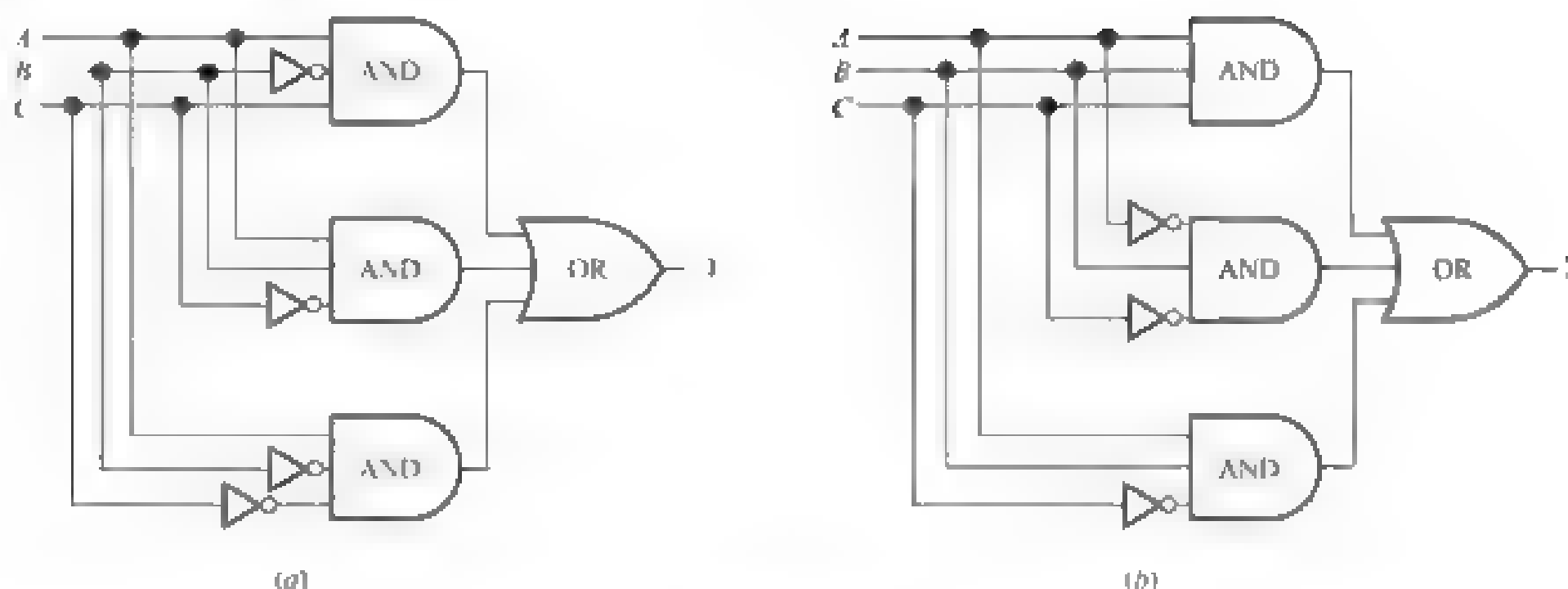



Figura 15-42

15.75 Suponha que três chaves *A*, *B* e *C* são conectadas à mesma lâmpada em um corredor. A qualquer momento, uma chave pode estar "para cima", denotado por 1, ou "para baixo", denotado por 0. Uma mudança em qualquer chave mudará a paridade (par ou ímpar) do número de 1's. As chaves serão capazes de controlar a luz se ela associar, digamos, uma natureza ímpar com a luz estando "ligada" (representado por 1) e uma natureza par com a luz estando "desligada" (representado por 0).

(a) Mostre que a tabela verdade a seguir satisfaz essas condições:

$$T(A, B, C) = T(00001111, 00110011, 01010101) = 01101001$$

(b) Desenhe um circuito mínimo *L* AND-OR com a tabela verdade acima.

Respostas dos Problemas Complementares

15.43 (a) $a + a'b = a + b$.

(b) $a \cdot 0 + a \cdot I = a$.

(c) $ab + bc = (a + c)b$.

15.45 (b) D_{55}: átomos 5 e 11. (d) D_{130}: átomos 2, 5 e 13.

15.46 (a) Existem oito elementos 1, 2, 5, 10, 11, 22, 55 e 110. Veja a Fig. 15-43(*a*).

(b) Existem cinco subálgebras: {1, 110}, {1, 2, 55, 110}, {1, 5, 22, 110}, {1, 10, 11, 110}, D_{110}.

(c) Existem 15 subreticulados que incluem as três subálgebras acima.

(d) $A = \{2, 5, 11\}$

(e) Veja a Fig. 15-43(*b*).

15.48 Maxtermos: 30, 42, 70 e 105

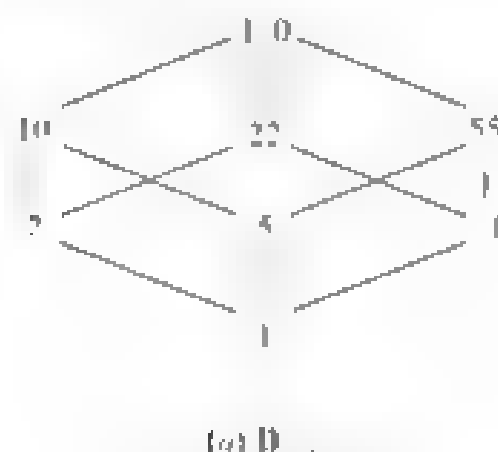



Figura 15-43

15.49 (b) *Sugestão:* Use dualidade.

15.53 (a) $xy'z$ (*b*) 0; (*c*) $xy'z't$; (*d*) 0

15.54 (a) $E = xy' + xy'z = xy'z' + xy'z$

(b) $E = xy + xz' = xyz + xyz' + xy'z'$.

(c) $E = xy' + y'z = xy'z + xy'z' + x'y'z$.

15.55 (a) $E = xyz' + x'y' = xyz' + x'y'z + x'y'z'$

(b) $E = x'y' = x'y'z + x'y'z'$.

(c) $E = x'yz'$

15.56 (a) $Q = xzt$. (b) $Q = xyt'$. (c) e (d) Não existe.

15.57 (a) $E_L = 11$, $E_S = 3$; (b) $E_L = 11$, $E_S = 4$.

15.58 (a) $x'y, x'z', y'z'$.

(b) $xy', xzt', y'zt', x'z't, y'z't$.

(c) $xyzt, xz't', y'z't', x'y'z, x'z't$.

15.59 (a) $E = x'y + x'z'$.

(b) $E = xy' + xzt' + x'z't + y'z't$.

(c) $E = xyzt + xz't' + x'y'z' + x'z't$.

15.60 (a) $Y = A'BC + A'C' + BC'$;

(b) $ABC + A'BC + AB'C'$.

15.61 (a) $Y = (AB')' + (A' + B + C)' + AC$

(b) $Y = (A'BC)' + A'BC' + (AB'C)' + AB'C'$

15.62 Veja a Fig. 15-44.

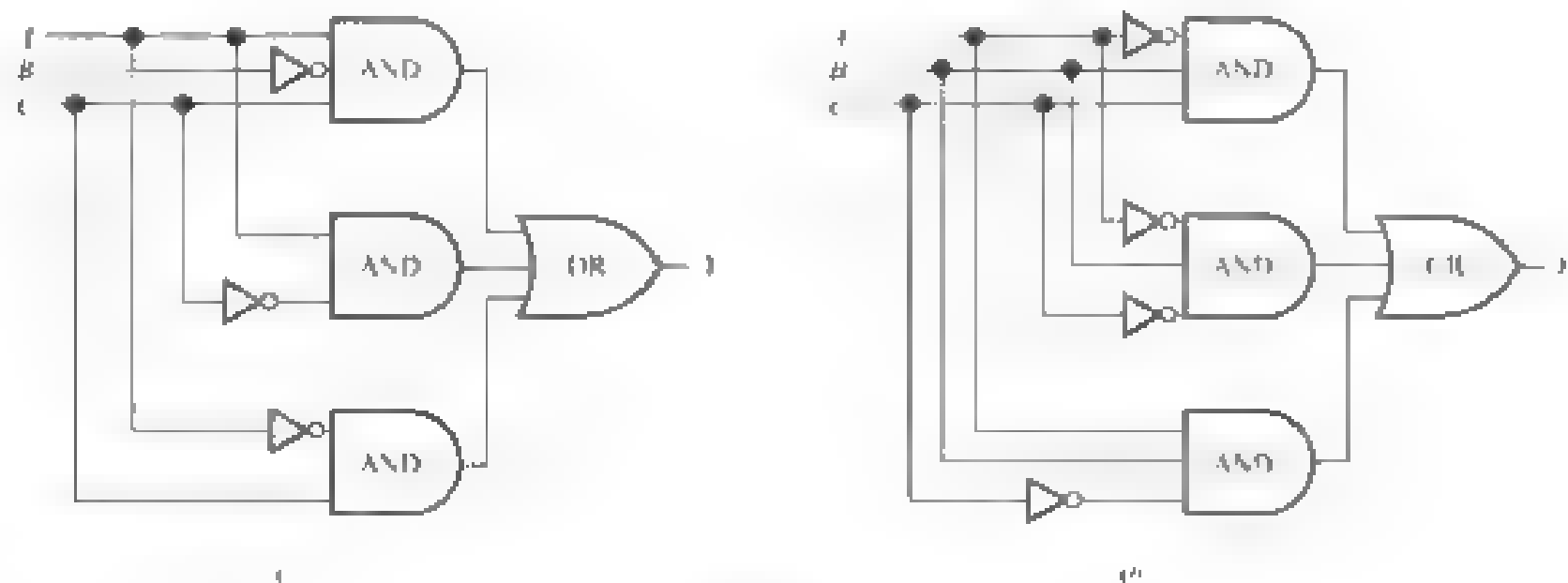



Figura 15-44

15.63 (a) $Y = 100001$, (b) $Y = 00111000$; (c) $Y = 00110000$.

15.64 (a) $Y = 100111$; (b) $Y = 10100111$, (c) $Y = 11111101$.

15.65 (a) $A' = 00011000$, (b) $A' = 01110111$, (c) $A' = 00000111$.

15.66 (a) $2^n = 2^6 = 64$.

(b) $x_1 = 000\ldots 00111\ldots 11$ (32 zeros) (32 uns).

$x_2 = (00000000000000001111111111111111)^2$.

$x_3 = (0000000011111111)^4$.

15.67 (a) $T(E) = 01010011$; (b) $T(E) = 00111111$.

15.68 (a) $T(E) = 01000000$; (b) $T(E) = 10001010$.

15.69 Use tabelas verdade para mintermos no Exemplo 15.13.

(a) $E = x'y'z' + x'yz + xyz'$

(b) $E = xy'z' + xyz$.

(c) $E = x'yz' + xyz'$

15.70 (a) $E = xy' + x'y + yz = xy' + x'y + xz'$

(b) $E = xy' + x'y + z$.

(c) $E = x' + z$.

15.71 (a) $E = x'y + zt' + xz't + xy'z$

$= x'y + zt' + xz't + xy't$.

(b) $E = yz + yt' + zt' + xy'z'$

(c) $E = x'y + yt + xy't' + x'zt$

$= x'y + yt + xy't' + y'zt$.

15.72 (a) $E = x' + y$; (b) $E = xz' + yz$.

15.73 (a) $E = y' + z't$; (b) $E = xy' + zt' + y'zt$

15.74 Veja a Fig. 15-45.

15.75 Veja a Fig. 15-46.

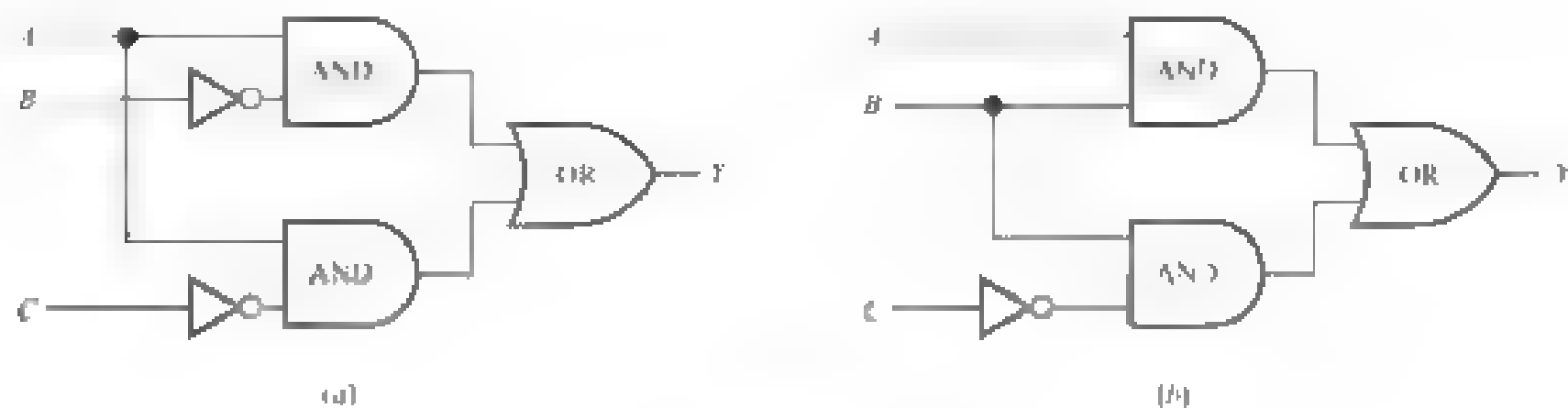



Figura 15-45

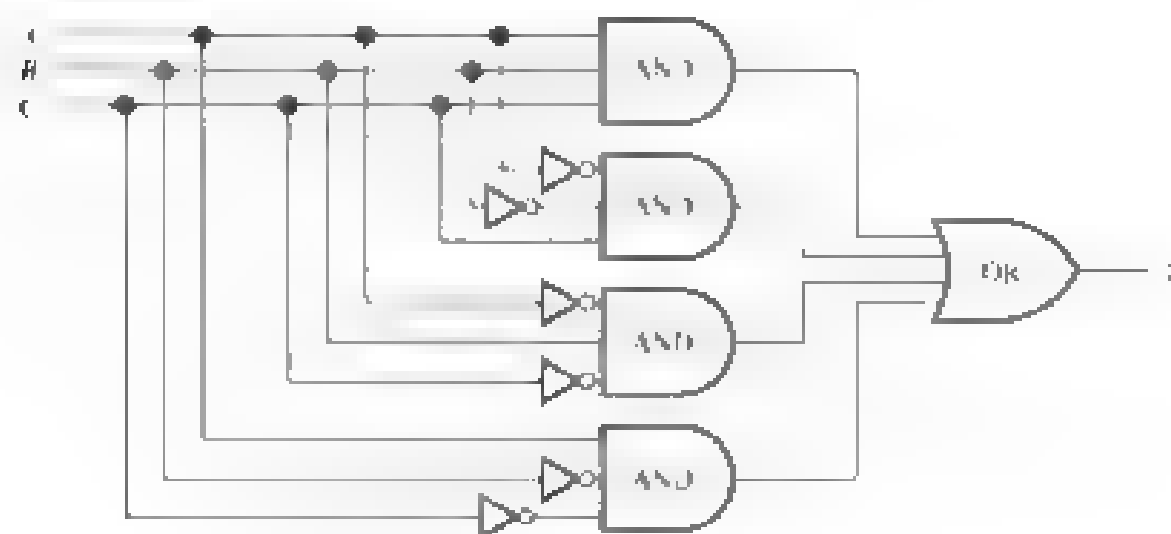



Figura 15-46

Vetores e Matrizes

A.1 INTRODUÇÃO

Dados são frequentemente distribuídos em *arrays*, isto é, conjuntos cujos elementos são indexados por um ou mais índices. Se esses dados consistem em números, então um array unidimensional é chamado de *vetor*, enquanto um array bidimensional é chamado de *matriz* (de forma que a dimensão denota o número de índices.) Este apêndice investiga esses vetores e matrizes e certas operações algébricas nas quais eles se envolvem. Nesse contexto, os números em si são chamados de *escalares*.

A.2 VETORES

Por *vetor u*, nós nos referimos a uma lista de números, como $a_1, a_2, \ldots, a_n$. Tal vetor é denotado por

$$u = (a_1, a_2, \ldots, a_n)$$

Os números a_i são chamados de *componentes* ou *entradas* de u. Se todos os $a_i = 0$, então u é chamado de *vetor nulo*. Dois desses vetores, u e v, são *iguais*, e escrevemos $u = v$, se possuem o mesmo número de componentes *e* esses componentes correspondentes são iguais.

Exemplo A.1

(a) Vetores em que os dois primeiros possuem dois componentes e os dois últimos possuem três componentes são os que se seguem.

$$(3, -4), \quad (6, 8), \quad (0, 0, 0), \quad (2, 3, 4)$$

O terceiro é o vetor nulo com três componentes.

(b) Apesar de os vetores (1, 2, 3) e (2, 3, 1) possuírem os mesmos números, não são iguais, uma vez que os componentes correspondentes não são iguais.

Operações vetoriais

Considere dois vetores arbitrários u e v com o mesmo número de componentes, por exemplo

$$u = (a_1, a_2, \ldots, a_n) \quad \text{e} \quad v = (b_1, b_2, \ldots, b_n)$$

A *soma* de u e v, que escrevemos na forma $u + v$, é o vetor obtido pela adição dos componentes correspondentes de u e v; isto é,

$$u + v = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

O *produto escalar*, ou simplesmente *produto*, de um escalar k e o vetor u, que escrevemos na forma ku, é o vetor obtido pela multiplicação de cada um dos componentes de u por k; isto é,

$$ku = (ka_1, ka_2, \ldots, ka_n)$$

Também definimos

$$-u = -1(u) \quad \text{e} \quad u - v = u + (-v)$$

e consideramos que 0 define o vetor nulo. O vetor $-u$ é chamado de *negativo* do vetor u.

O *produto interno* dos vetores u e v acima é denotado e definido por

$$u \cdot v = a_1b_1 + a_2b_2 + \cdots + a_nb_n$$

O *comprimento* do vetor u é definido por

$$\|u\| = \sqrt{u \cdot u} = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$$

Apontamos que $\|u\| = 0$ se, e somente se, $u = 0$; caso contrário, $\|u\| > 0$.

Exemplo A.2 Seja $u = (2, 3, -4)$ e $v = (1, -5, 8)$. Então

$$u + v = (2 + 1, 3 - 5, -4 + 8) = (3, -2, 4)$$
$$5u = (5 \cdot 2, 5 \cdot 3, 5 \cdot (-4)) = (10, 15, -20)$$
$$-v = -1 \cdot (1, -5, 8) = (-1, 5, -8)$$
$$2u - 3v = (4, 6, -8) + (-3, 15, -24) = (1, 21, -32)$$
$$u \cdot v = 2 \cdot 1 + 3 \cdot (-5) + (-4) \cdot 8 = 2 - 15 - 32 = -45$$
$$\|u\| = \sqrt{2^2 + 3^2 + (-4)^2} = \sqrt{4 + 9 + 16} = \sqrt{29}$$

Vetores sob as operações de adição vetorial e multiplicação escalar possuem várias propriedades, por exemplo,

$$k(u + v) = ku + kv$$

onde k é um escalar e u e v são vetores. Muitas dessas propriedades aparecem no Teorema A.1, que também é válido para vetores, uma vez que estes podem ser vistos como um caso particular de matrizes.

Vetores coluna

Às vezes, uma lista de vetores é escrita verticalmente em vez de horizontalmente, e essa lista é chamada de *vetor coluna*. Nesse contexto, os vetores acima escritos horizontalmente são chamados de *vetores linha*. As operações acima para vetores linha são definidas analogamente para vetores coluna.

A.3 MATRIZES

Uma *matriz A* é um array retangular de números, usualmente representada na forma

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

As m listas horizontais de números são chamadas de *linhas* de A, e as n listas verticais de números são suas *colunas*. Logo, o elemento a_{ij}, chamado de *entrada ij*, aparece na linha i e coluna j. Frequentemente, denotamos tal matriz escrevendo apenas $A = [a_{ij}]$.

Uma matriz com m linhas e n colunas é chamada de uma matriz m por n, escrita na forma $m \times n$. O par de números m e n é chamado de *tamanho* da matriz. Duas matrizes A e B são iguais, que é escrito na forma $A = B$, se elas possuem o mesmo tamanho e se os elementos correspondentes forem iguais. Logo, a igualdade de duas matrizes $m \times n$ é equivalente a um sistema de mn igualdades, uma para cada um dos pares correspondentes de elementos.

Uma matriz com apenas uma linha é chamada de *matriz linha* ou *vetor linha*, e uma matriz com apenas uma coluna é chamada de *matriz coluna* ou *vetor coluna*. Uma matriz cujas entradas são todas zero, é chamada de *matriz nula* e é usualmente denotada por 0.

Exemplo A.3

(a) O array retangular $A = \begin{bmatrix} 1 & -4 & 5 \\ 0 & 3 & 2 \end{bmatrix}$ é uma matriz 2×3. Suas linhas são $[1, -4, 5]$ e $[0, 3, -2]$ e suas colunas são $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -4 \\ 3 \end{bmatrix}, \begin{bmatrix} 5 \\ -2 \end{bmatrix}$.

(b) A matriz nula 2×4 é $0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

(c) Suponha que

$$\begin{bmatrix} x+y & 2z+t \\ x-y & z-t \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 5 \end{bmatrix}$$

Então as quatro entradas correspondentes precisam ser iguais. Isto é,

$$x+y=3, \quad x-y=1, \quad 2z+t=7, \quad z-t=5$$

A solução para o sistema de equações é

$$x=2, \quad y=1, \quad z=4, \quad t=-1$$

A.4 ADIÇÃO DE MATRIZES E MULTIPLICAÇÃO ESCALAR

Sejam $A = [a_{ij}]$ e $B = [b_{ij}]$ duas matrizes do mesmo tamanho, digamos, $m \times n$. A *soma* de A e B, escrita na forma $A + B$, é a matriz obtida pela adição dos elementos correspondentes de A e B. O *produto* (*escalar*) da matriz A por um escalar k, escrito na forma kA, é a matriz obtida pela multiplicação de cada elemento de A por k. Essas operações são denotadas na Fig. A-1.

$$A+B = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{bmatrix} \quad \text{e} \quad kA = \begin{bmatrix} ka_{11} & ka_{12} & \cdots & ka_{1n} \\ ka_{21} & ka_{22} & \cdots & ka_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ ka_{m1} & ka_{m2} & \cdots & ka_{mn} \end{bmatrix}$$

Figura A-1

Observe que $A + B$ e kA são também matrizes $m \times n$. Também definimos

$$-A = (-1)A \quad \text{e} \quad A - B = A + (-B)$$

A matriz $-A$ é chamada de *negativa* de A. A soma de matrizes com diferentes tamanhos não é definida.

Exemplo A.4 Considere que $A = \begin{bmatrix} 1 & -2 & 3 \\ 0 & 4 & 5 \end{bmatrix}$ e $B = \begin{bmatrix} 4 & 6 & 8 \\ 1 & 3 & 7 \end{bmatrix}$. Então

$$A + B = \begin{bmatrix} 1+4 & -2+6 & 3+8 \\ 0+1 & 4+(-3) & 5+(-7) \end{bmatrix} = \begin{bmatrix} 5 & 4 & 11 \\ 1 & 1 & -2 \end{bmatrix}$$

$$3A = \begin{bmatrix} 3(1) & 3(-2) & 3(3) \\ 3(0) & 3(4) & 3(5) \end{bmatrix} = \begin{bmatrix} 3 & -6 & 9 \\ 0 & 12 & 15 \end{bmatrix}$$

$$2A - 3B = \begin{bmatrix} 2 & -4 & 6 \\ 0 & 8 & 10 \end{bmatrix} + \begin{bmatrix} -12 & -18 & -24 \\ -3 & -9 & -21 \end{bmatrix} = \begin{bmatrix} -10 & -22 & -18 \\ -3 & 17 & 31 \end{bmatrix}$$

Matrizes no processo de adição e multiplicação escalar possuem as seguintes propriedades.

Teorema A.1: Sejam A, B e C matrizes com o mesmo tamanho, e considere que k e k' são escalares. Então:

(i) $(A + B) + C = A + (B + C)$

(ii) $A + 0 = 0 + A$

(iii) $A + (-A) = (-A) + 0 = A$

(iv) $A + B = B + A$

(v) $k(A + B) = kA + kB$

(vi) $(k + k')A = kA + k'A$

(vii) $(kk')A = k(k'A)$

(viii) $1A = A$

Note, em primeiro lugar, que o 0 em (ii) e (iii) refere-se à matriz nula. Além disso, segundo (i) e (iv), qualquer soma de matrizes

$$A_1 + A_2 + \cdots + A_n$$

Não requer parênteses e a soma não depende da ordem das matrizes. Fora isso, usando (vi) e (viii), temos também

$$A + A = 2A, \quad A + A + A = 3A, \quad \ldots$$

Por último, uma vez que vetores de n componentes podem ser identificados com matrizes $1 \times n$ ou $n \times 1$, o Teorema A.1 também é válido para vetores sob adição vetorial e multiplicação escalar.

A demonstração do Teorema A.1 se reduz a mostrar que as entradas ij em ambos os lados de cada uma das equações da matriz são iguais.

A.5 MULTIPLICAÇÃO DE MATRIZES

O produto das matrizes A e B, escrito na forma AB, é um pouco complicado. Por essa razão, comecemos com um caso particular. (O leitor é direcionado à Seção 3.5 para uma discussão do símbolo de somatória Σ, a letra grega maiúscula sigma.)

O produto AB de uma matriz linha $A = [a_i]$ e uma matriz coluna $B = [b_i]$ com o mesmo número de elementos é definido como se segue:

$$AB = [a_1, a_2, \ldots, a_n]\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = a_1b_1 + a_2b_2 + \cdots + a_nb_n = \sum_{k=1}^{n} a_kb_k$$

O produto AB é obtido pela multiplicação das entradas correspondentes em A e B e, então, somando todos os produtos. Enfatizamos que AB é um escalar (ou uma matriz 1×1). O produto AB não é definido quando A e B possuem um número diferente de elementos.

Exemplo A.5

(a) $[6, -4, 5]\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} = 7(3) + (-4)(2) + 5(-1) = 21 - 8 - 5 = 8$

(b) $[6, -1, 8, 3]\begin{bmatrix} 4 \\ -9 \\ -2 \\ 5 \end{bmatrix} = 24 + 9 - 16 + 15 = 32$

Agora estamos prontos para definir a multiplicação de matrizes em geral

Definição A.1: Sejam $A = [a_{ik}]$ e $B = [b_{kj}]$ matrizes, tal que o número de colunas de A é igual ao número de linhas de B, por exemplo, A é uma matriz $m \times p$ e B é uma matriz $p \times n$. Então o produto AB é a $m \times n$ matriz $C = [c_{ij}]$ cuja entrada ij é obtida pela multiplicação da i-ésima linha de A pela j-ésima coluna de B, isto é,

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj} = \sum_{k=1}^{p} a_{ik}b_{kj}$$

O produto AB é denotado na Fig. A-2.

$$\begin{bmatrix} a_{11} & \cdots & a_{1p} \\ \cdot & \cdots & \cdot \\ a_{i1} & \cdots & a_{ip} \\ \cdot & \cdots & \cdot \\ a_{m1} & \cdots & a_{mp} \end{bmatrix} \begin{bmatrix} b_{11} & \cdots & b_{1j} & \cdots & b_{1n} \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ b_{p1} & \cdots & b_{pj} & \cdots & b_{pn} \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \cdot & \cdots & \cdot \\ \cdot & c_{ij} & \cdot \\ \cdot & \cdots & \cdot \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}$$

Figura A-2

Enfatizamos que o produto AB não é definido se A for uma matriz $m \times p$ e se B for $q \times n$ onde $p \neq q$.

Exemplo A.6

(a) Encontre AB onde $A = \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ e $B = \begin{bmatrix} 2 & 0 & -4 \\ 5 & -2 & 6 \end{bmatrix}$.

Uma vez que A é 2×2 e B é 2×3, o produto AB é definido e é uma matriz 2×3. Para obter a primeira linha da matriz produto AB, multiplique a primeira linha (1, 3) de A pelas colunas de B,

$$\begin{bmatrix} 2 \\ 5 \end{bmatrix}, \begin{bmatrix} 0 \\ -2 \end{bmatrix}, \begin{bmatrix} -4 \\ 6 \end{bmatrix}$$

respectivamente. Isto é,

$$AB = [2 + 15 \quad 0 - 6 \quad -4 + 18] = [17 \quad -6 \quad 14]$$

Para obter a segunda linha do produto AB, multiplique a segunda linha (2, −1) de A pelas colunas de B, respectivamente. Então

$$AB = \begin{bmatrix} 17 & -6 & 14 \\ 4-5 & 0+2 & -8-6 \end{bmatrix} = \begin{bmatrix} 17 & -6 & 14 \\ -1 & 2 & -14 \end{bmatrix}$$

(b) Suponha que $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix}$. Então

$$AB = \begin{bmatrix} 5+0 & 6-4 \\ 15+0 & 18 \quad 8 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 15 & 10 \end{bmatrix} \quad \text{e} \quad BA = \begin{bmatrix} 5+18 & 10+24 \\ 0 \quad 6 & 0 \quad 8 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ 6 & 8 \end{bmatrix}$$

O Exemplo A.6(b) acima mostra que a multiplicação de matrizes não é comutativa, isto é, que os produtos AB e BA de matrizes não precisam ser iguais.

A multiplicação de matrizes satisfaz, no entanto, as propriedades a seguir:

Teorema A.2: Sejam A, B e C matrizes. Então, quando os produtos e somas são definidos

(i) $(AB)C = A(BC)$ (Lei Associativa)

(ii) $A(B + C) = AB + AC$ (Lei da Distribuição da Esquerda)

(iii) $(B + C)A = BA + CA$ (Lei da Distribuição da Direita)

(iv) $k(AB) = (kA)B = A(kB)$ quando k é um escalar.

Multiplicação de matrizes e sistemas de equações lineares

Qualquer sistema S de equações lineares é equivalente à equação matricial

$$AX = B$$

Quando A é a matriz que consiste nos coeficientes, X é o vetor coluna de valores desconhecidos e B é o vetor coluna de constantes. (Aqui, *equivalente* significa que qualquer solução do sistema S é também uma solução da equação matricial $AX = B$, e vice-versa.) Por exemplo, o sistema

$$\begin{array}{r} x + 2y - 3z = 4 \\ 5x - 6y + 8z = 9 \end{array} \quad \text{é equivalente a} \quad \begin{bmatrix} 1 & 2 & -3 \\ 5 & -6 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 4 \\ 9 \end{bmatrix}$$

Observe que o sistema é completamente determinado pela matriz

$$M = [A, B] = \begin{bmatrix} 1 & 2 & -3 & 4 \\ 5 & -6 & 8 & 9 \end{bmatrix}$$

que é chamada de *matriz aumentada* do sistema.

A.6 TRANSPOSTA

A *transposta* da matriz A, escrita na forma A^T, é a matriz obtida pela escrita das linhas de A, em ordem, na forma de colunas. Por exemplo,

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix} \quad \text{e} \quad [1, -3, -5]^T = \begin{bmatrix} 1 \\ -3 \\ -5 \end{bmatrix}$$

Note que, se A é uma matriz $m \times n$, então A^T é uma matriz $m \times n$. Em particular, a transposta de um vetor linha é um vetor coluna, e vice-versa. Além disso, se $B = [b_{ij}]$ é a transposta de $A = [a_{ij}]$, então $b_{ij} = a_{ji}$ para todo i e todo j.

A.7 MATRIZES QUADRADAS

Uma matriz com o mesmo número de linhas e colunas é chamada de *matriz quadrada*. Uma matriz quadrada com n linhas e colunas é dita de *ordem* n e é chamada de *matriz n-quadrada*.

A *diagonal principal*, ou apenas *diagonal*, de uma matriz n-quadrada $A = [a_{ij}]$ consiste nos elementos a_{11}, $a_{22}, \ldots, a_{nn}$, isto é, os elementos do canto esquerdo superior até o canto direito inferior da referida matriz. O *traço* de A, escrito na forma $\text{tr}(A)$, é a soma dos elementos da diagonal, isto é, $\text{tr}(A) = a_{11} + a_{22} + \cdots + a_{nn}$.

A *matriz unitária* n-quadrada, denotada por I_n, ou apenas I, é a matriz quadrada com apenas 1's na diagonal e 0's no resto dela. A matriz unitária I tem o mesmo papel em multiplicação de matrizes que o número 1 na multiplicação usual de números. Especificamente, para qualquer matriz A,

$$AI = IA = A$$

Considere, por exemplo, as matrizes

$$\begin{bmatrix} 1 & -2 & 0 \\ 0 & -4 & -6 \\ 5 & 3 & 2 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Ambas são matrizes quadradas. A primeira é de ordem 3 e sua diagonal consiste nos elementos 1, −4 e 2, então seu traço é igual a $1 - 4 + 2 = -1$. A segunda matriz é de ordem 4, sua diagonal consiste apenas em 1's e o restante dela é formado de 0's. Logo, a segunda matriz é a matriz unitária de ordem 4.

Álgebra de matrizes quadradas

Seja A uma matriz quadrada qualquer. Então podemos multiplicar A por ela mesma. Na verdade, podemos formar todas as *potências* não negativas de A como se segue.

$$A^2 = AA, \quad A^3 = A^2A, \ldots, \quad A^{n+1} = A^nA, \ldots, \quad \text{e} \quad A^0 = I \text{ (quando } A \neq 0)$$

Polinômios na matriz A também são definidos. Especificamente, para qualquer polinômio

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

Onde os a_i são escalares, definimos $f(A)$ como sendo a matriz.

$$f(A) = a_0I + a_1A + a_2A^2 + \cdots + a_nA^n$$

Note que $f(A)$ é obtido por $f(x)$, por meio da substituição da matriz A pela variável x e substituindo a matriz escalar a_0I pelo termo escalar a_0. No caso em que $f(A)$ é a matriz nula, a matriz A é, então, chamada de *zero* ou *raiz* do polinômio $f(x)$.

Exemplo A.7 Suponha que $A = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}$. Então

$$A^2 = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 7 & -6 \\ 9 & 22 \end{bmatrix} \quad \text{e}$$

$$A^3 = A^2A = \begin{bmatrix} 7 & 6 \\ -9 & 22 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} 11 & 38 \\ 57 & -106 \end{bmatrix}$$

Suponha que $f(x) = 2x^2 - 3x + 5$. Então

$$f(A) = 2\begin{bmatrix} 7 & 6 \\ -9 & 22 \end{bmatrix} - 3\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 16 & 18 \\ 27 & 61 \end{bmatrix}$$

Suponha que $g(x) = x^2 + 3x - 10$. Então

$$g(A) = \begin{bmatrix} 7 & 6 \\ 9 & 22 \end{bmatrix} + 3\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} - 10\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Logo, A é um zero do polinômio $g(x)$.

A.8 MATRIZES INVERSÍVEIS (NÃO SINGULARES) E INVERSOS

Uma matriz quadrada A é dita *inversível*, (ou *não singular*) se existir uma matriz B tal que

$$AB = BA = I, \text{ (a matriz identidade).}$$

Tal matriz B é única, ela é chamada de *inversa* de A e denotada por A^{-1}. Observe que B é a inversa de A se, e somente se, A for a inversa de B. Por exemplo, suponha que

$$A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$$

Então

$$AB = \begin{bmatrix} 6-5 & -10+10 \\ 3-3 & -5+6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{e} \quad BA = \begin{bmatrix} 6-5 & 15-15 \\ -2+2 & -5+6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Logo, A e B são inversos.

É sabido que $AB = I$ se, e somente se, $BA = I$; portanto, só é necessário testar um produto para determinar se duas matrizes são inversas. Por exemplo,

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix} \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix} = \begin{bmatrix} -11+0+12 & 2+0-2 & 2+0-2 \\ -22+4+18 & 4+0-3 & 4-1-3 \\ -44-4+48 & 8+0-8 & 8+1-8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Logo, as duas matrizes são inversíveis e são inversas uma da outra.

A.9 DETERMINANTES

Para cada matriz n-quadrada $A = [a_{ij}]$, associamos um número específico chamado de *determinante* de A, que é denotado por $\det(A)$, $|A|$ ou

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

Enfatizamos que um array quadrado de números cercados por linhas retas, chamado de *determinante de ordem n*, não é uma matriz, mas denota o número que a função determinante associa a esse array fechado de números, isto é, a matriz quadrada fechada.

Os determinantes de ordem 1, 2 e 3 são definidos como se segue.

$$|a_{11}| = a_{11} \qquad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

O diagrama na Fig. A-3(a) pode ajudar o leitor a lembrar o determinante de ordem 2. Isto é, o determinante é igual ao produto dos elementos ao longo da flecha marcada com o símbolo de +, subtraindo o produto dos elementos ao longo da flecha marcada com o símbolo de −. Existe um diagrama análogo para ajudar a lembrar o determinante de ordem 3 que aparece na Fig. A-3(b). Por uma questão de conveniência para a notação, separamos as três flechas com símbolo de + e as três com símbolo de −. Enfatizamos ainda que não existem truques diagramáticos para ajudar a lembrar os determinantes de maior ordem.

(a) (b)

Figura A-3

Exemplo A.8

(a) $\begin{vmatrix} 5 & 4 \\ 2 & 3 \end{vmatrix} = 5(3) - 4(2) = 15 - 8 = 7$, $\begin{vmatrix} 2 & 1 \\ 4 & 6 \end{vmatrix} = 2(6) - 1(-4) = 12 + 4 = 16$.

(b) $\begin{vmatrix} 2 & 1 & 3 \\ 4 & 6 & -1 \\ 5 & 1 & 0 \end{vmatrix} = 2(6)(0) + 1(-1)(5) + 3(1)(4) - 5(6)(3) - 1(-1)(2) - 0(1)(4)$

$= 0 - 5 + 12 - 90 + 2 - 0 = 81$

Definição geral de determinantes

A definição geral de um determinante de ordem n é como se segue:

$$\det(A) = \sum \operatorname{sgn}(\sigma) a_{1j_1} a_{2j_2} \cdots a_{nj_n}$$

onde a soma é aplicada sobre todas as permutações $\sigma = \{j_1, j_2, \ldots, j_n\}$ de $\{1, 2, \ldots, n\}$. Aqui, $\operatorname{sgn}(\sigma)$ é igual a $+1$ ou -1, de acordo com um número par ou ímpar de trocas que são necessárias para mudar σ, de modo que seus números estejam na ordem usual. Incluímos a definição geral da função determinante por uma questão de completude. O leitor deve consultar textos sobre teoria de matrizes ou álgebra linear para técnicas de cálculo de determinantes de ordem superior a três. Permutações são estudadas no Capítulo 5.

Uma propriedade importante da função determinante é de que ela é multiplicativa. Isto é:

Teorema A.3: Sejam A e B duas matrizes n-quadradas quaisquer. Então

$$\det(AB) = \det(A) \cdot \det(B)$$

A demonstração do teorema acima está além do objetivo deste texto.

Determinantes e inversas de matrizes 2 × 2

Considere uma matriz 2 × 2 arbitrária $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Suponha que $|A| = ad - bc \neq 0$. Então é possível provar que

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix} = \frac{1}{|A|}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Em outras palavras, quando $|A| \neq 0$, a inversa de uma matriz A 2 × 2 é obtida como se segue:

(1) Troca de elementos na diagonal principal

(2) Considere os negativos dos outros elementos.

(3) Multiplique a matriz por $1/|A|$ ou, de forma equivalente, divida cada elemento por $|A|$

Por exemplo, se $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$, então $|A| = -2$ e, portanto,

$$A^{-1} = \frac{1}{-2}\begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} -\frac{5}{2} & \frac{3}{2} \\ 2 & -1 \end{bmatrix}$$

Por outro lado, se $|A| = 0$, então A^{-1} não existe. Apesar de não existir uma fórmula simples para matrizes de ordem superior, esse resultado é geralmente válido.

Teorema A.4: Uma matriz A é inversível se, e somente se, possuir um determinante diferente de zero.

A.10 OPERAÇÕES ELEMENTARES SOBRE LINHAS, ELIMINAÇÃO GAUSSIANA (OPCIONAL)

Esta seção discute o algoritmo de eliminação Gaussiana no contexto de operações elementares sobre linhas.

Operações elementares de linhas

Considere uma matriz $A = [a_{ij}]$ cujas linhas serão denotadas, respectivamente, por $R_1, R_2, \ldots, R_m$. O primeiro elemento diferente de zero em uma linha R_i é chamado de elemento *principal* diferente de zero. Uma linha inteiramente de zeros é chamada de *linha nula*. Logo, uma linha nula não possui elemento principal diferente de zero.

As três operações em A a seguir são chamadas de *operações elementares de linha*:

[E_1] Permute as linhas R_i e R_j. Essa operação será indicada, escrevendo: "Permute R_i e R_j."

[E_2] Multiplique cada elemento em uma linha R_i por uma constante k diferente de zero. Essa operação será indicada, escrevendo: "Multiplique R_i por k."

[E_3] Some um múltiplo de uma linha R_i à outra R_j ou, em outras palavras, substitua R_j pela soma $kR_i + R_j$. Essa operação será indicada, escrevendo: "Some kR_i a R_j."

Para evitar frações, fazemos [E_2] e [E_3] em apenas um passo, isto é, aplicamos as seguintes operações:

[E] Some um múltiplo de uma linha R_i a um múltiplo diferente de zero de outra linha R_j ou, em outras palavras, substitua R_j pela soma $kR_i + k'R_j$ onde $k' \neq 0$. Indicamos essa operação, escrevendo: "Some kR_i a $k'R_j$."

Enfatizamos que, nas operações de linha [E_3] e [E], apenas a linha R_j é, de fato, alterada.

Notação: Matrizes A e B são ditas *linha-equivalentes*, escrito na forma $A \sim B$, se a matriz B pode ser obtida a partir da matriz A, ao se usar operações elementares de linhas.

Matrizes escada

Uma matriz A é chamada de *matriz escada*, ou estando na *forma escada*, se as duas condições a seguir forem válidas:

(i) Todas as linhas nulas, se existirem, estão na parte inferior da matriz.

(ii) Cada entrada principal diferente de zero está à direita da entrada principal diferente de zero na linha precedente.

A matriz é dita na *forma canônica de linhas* se possuir as duas propriedades adicionais:

(iii) Cada entrada principal diferente de zero será igual a 1.

(iv) Cada entrada principal diferente de zero é a única entrada diferente de zero em sua coluna.

A matriz nula 0, para qualquer número de colunas, é um exemplo especial de uma matriz em forma canônica de linhas. A matriz identidade n-quadrada I_n é outro exemplo de uma matriz em forma canônica de linhas.

Uma matriz quadrada A é dita na *forma triangular* se suas entradas diagonais $a_{11}, a_{22}, \ldots, a_{nn}$ são as entradas principais diferentes de zero. Logo, uma matriz quadrada em forma triangular é um caso especial de uma matriz escada. A matriz identidade I é o único exemplo de matriz quadrada que está em forma triangular e também em forma canônica de linhas.

Exemplo A.9 Considere as matrizes escada na Fig. A-4 cujas entradas principais diferentes de zero foram demarcadas por um círculo. (Os zeros precedendo e abaixo das entradas principais diferentes de zero em uma matriz escada formam uma padrão em forma de "escada", como indicado a seguir pelo escurecimento das demais entradas.) A terceira matriz está na forma canônica de linha. A segunda matriz não está na forma canônica de linha, uma vez que a terceira coluna contém uma entrada principal diferente de zero junto de outra entrada diferente de zero. A primeira matriz não está na forma canônica, uma vez que algumas das entradas principais diferentes de zero não são 1. A última matriz está na forma triangular.

$$\begin{bmatrix} \textcircled{2} & 3 & 2 & 0 & 4 & 5 & -6 \\ 0 & 0 & \textcircled{1} & 1 & 3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \textcircled{6} & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \textcircled{1} & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & \textcircled{1} & 3 & 0 & 0 & 4 \\ 0 & 0 & 0 & \textcircled{1} & 0 & 3 \\ 0 & 0 & 0 & 0 & \textcircled{1} & 2 \end{bmatrix} \begin{bmatrix} \textcircled{2} & 4 & 7 \\ 0 & 5 & 8 \\ 0 & 0 & \textcircled{6} \end{bmatrix}$$

Figura A-4

Eliminação Gaussiana em forma de matriz

Considere qualquer matriz A. Dois algoritmos, A-1 e A-2, são apresentados nas Fig. A-5 e Fig. A-6, respectivamente. O primeiro algoritmo transforma a matriz A em forma de escada (usando apenas operações elementares de linha) e o segundo transforma a matriz escada na forma canônica de linhas. (Os dois algoritmos juntos são chamados de *eliminação Gaussiana*.)

No fim do Algoritmo A-1, as entradas *pivô* (principal diferente de zero) serão

$$a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r}$$

onde r denota o número de linhas diferentes de zero na matriz em forma escada.

Observação 1: O número $m = \dfrac{a_{ij_1}}{a_{1j_1}} = \dfrac{\text{coeficiente a ser deletado}}{\text{pivô}}$ é chamado de *multiplicador*.

Observação 2: É possível substituir a operação no Passo 1 (*b*) por

$$\text{“Some } -a_{ij_1}R_1 \text{ a } a_{1j_1}R_i\text{”}$$

Isso evitaria frações se todos os escalares fossem, originalmente, inteiros.

Exemplo A.10 Encontre a forma canônica de linhas de $A = \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 2 & 4 & 4 & 6 & 10 \\ 3 & 6 & -6 & 9 & 13 \end{bmatrix}$

Primeiro reduza A à forma escada usando o Algoritmo A-1. Especificamente, use $a_{11} = 1$ como um pivô para obter zeros abaixo de a_{11}, isto é, aplique as operações de linha “Some $-2R_1$ a R_2” e “Some $-3R_1$ a R_3”. Então use $a_{23} = 2$ como um pivô para obter 0 abaixo de a_{23}, isto é, aplique a operação de linha “Some $-\frac{3}{2}R_2$ a R_3”. Isso implica

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 3 & 6 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}$$

A matriz A está agora na forma escada.

Agora use o Algoritmo A-2 para reduzir A para a forma canônica de linha. Especificamente, multiplique R_3 por $-1/2$ de forma que a entrada pivô $a_{35} = 1$, então use $a_{35} = 1$ como um pivô para obter zeros acima dele por meio das operações “Some $-6R_3$ a R_2” e “Some $-2R_3$ a R_1”. Isso implica:

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 0 \\ 0 & 0 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Multiplique R_2 por $\frac{1}{2}$ de forma que a entrada pivô $a_{23} = 1$, então use $a_{23} = 1$ como um pivô para obter 0 acima dele por meio da operação “Some $3R_2$ a R_1”. Isso implica.

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 7 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A última matriz é a forma canônica de linha de A.

Algoritmo A-1: (Eliminação para a frente): A entrada é uma matriz arbitrária $A = [a_{ij}]$.

Passo 1. Encontre a primeira coluna com uma entrada diferente de zero. Se tal coluna não existir, então SAÍDA. (Temos a matriz zero.) Caso contrário, considere j_1 a notação do número dessa coluna.

(*a*) Arranje de forma que $a_{1j_1} \neq 0$. Isto é, se necessário, permute linhas de modo que uma entrada diferente de zero apareça na primeira linha na coluna j_1.

(*b*) Use a_{1j_1} como um *pivô* para obter zeros abaixo de a_{1j_1}. Isto é, para $i > 1$:

(1) Considere $m = -a_{ij_1}/a_{1j_1}$.
(2) Some mL_1 a L_i.

(Isso substitui a linha R_i por $-(a_{ij_1}/a_{1j_1})R_1 + R_i$.)

Passo 2. Repita o passo um com a submatriz formada por todas as linhas, excluindo a primeira. Aqui assumimos que j_2 denota a primeira coluna na submatriz com uma entrada diferente de zero. Portanto, no final do Passo 2, temos $a_{2j_2} \neq 0$.

Passo 3 para r + 1. Continue o processo acima até que a submatriz não possua nenhuma entrada diferente de zero.

Figura A-5

O Passo r final no Algoritmo A-2 na Fig. A-6 transforma o primeiro pivô em 1.

Algoritmo A-2. (Eliminação para trás): A entrada é uma matriz $A = [a_{ij}]$ na forma escada com entradas pivô $a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r}$.

Passo 1. (*a*) Multiplique a última linha diferente de zero R_r por $1/a_{rj_r}$ de modo que a entrada pivô seja igual a 1.

(*b*) Use $a_{rj_r} = 1$ para obter zeros acima do pivô. Isto é, para $i = r-1, r-2, \ldots, 1$:

(1) Considere que $m = -a_{ij_r}$
(2) Some mR_r a R_i.

Em outras palavras, aplique as operações elementares de linha

$$\text{“Some } -a_{ir_1} R_r \text{ a } R_i\text{”}$$

(Isso substitui a linha R_i por $-a_{ir_i}R_r + R_i$.)

Passo 2 para r − 1. Repita o Passo 1 para as linhas $R_{r-1}, R_{r-2}, \ldots, R_2$.

Passo r. Multiplique R_1 por $1/a_{1j_1}$.

Figura A-6

Os Algoritmos A-1 e A-2 mostram que qualquer matriz é equivalente em suas linhas a, pelo menos, uma matriz em forma canônica de linha. Na verdade, é possível provar na álgebra linear que tal matriz é única, é chamada de *forma canônica de linha* de *A*.

Teorema A.5: Qualquer matriz A é linha-equivalente a uma matriz única na forma canônica de linhas.

Solução matricial de um sistema linear de equações

Considere um sistema S de equações lineares ou, de forma equivalente, uma equação matricial $AX = B$ com a matriz aumentada $M = [A, B]$. O sistema é resolvido na aplicação do algoritmo e eliminação Gaussiana acima em M, como se segue.

Parte A (*Redução*): Reduza a matriz M aumentada para a forma escada. Se uma linha da forma $(0, 0, \ldots, 0, b)$, com $b \neq 0$, aparecer, então *pare*. O sistema não possui solução.

Parte B (*Substituição retroativa*): Reduza ainda mais a matriz aumentada M para sua forma canônica de linha.

A solução única do sistema ou, quando a solução não é única, a forma de variável livre da solução é facilmente obtida a partir da forma canônica de linha de M.

O exemplo a seguir se aplica ao algoritmo recém-dado a um sistema S com uma solução única. Os casos onde S não possui solução e onde S possui um número infinito de soluções são mostrados no Problema A.23.

Exemplo A.11

Resolva o sistema: $\begin{cases} x + 2y + z = 3 \\ 2x + 5y - z = -4 \\ 3x - 2y - z = 5 \end{cases}$

Reduza sua matriz aumentada M para a forma escada e então para a forma canônica de linhas como se segue

$$M = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & 5 & -1 & -4 \\ 3 & -2 & -1 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & -8 & -4 & -4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & 3 & 10 \\ 0 & 0 & -28 & -84 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & 3 & 10 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

Logo, o sistema possui a solução única $x = 2$, $y = -1$, $z = 3$ ou, de forma equivalente, o vetor $u = (2, -1, 3)$. Notamos que a forma escada de M já indica que a solução é única, uma vez que ela corresponde a um sistema triangular.

Inversa de uma matriz $n \times n$

A Figura A-7 contém o Algoritmo A-3 que encontra a inversa A^{-1} de qualquer matriz $n \times n$ arbitrária.

Algoritmo A-3: Encontre a inversa de uma matriz A $n \times n$.

Passo 1. Forme a $n \times 2n$ matriz $M = [A, I]$, isto é, A está na metade esquerda de M, e a matriz identidade I está na metade direita.

Passo 2. Reduza as linhas de M para a forma escada. Se o processo gerar uma linha erro na metade de A de M, então *pare* (A não possui inversa). Caso contrário, a metade A está agora na forma triangular

Passo 3. Reduza ainda mais as linhas de M para a forma canônica de linha

$$M \sim [I, B]$$

onde I substitui A na metade esquerda de M.

Passo 4. Assuma que $A^{-1} = B$, onde B é a matriz que está agora na metade direita de M.

Figura A-7

Exemplo A.12

Encontre a inversa de $A = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 3 \\ 4 & 1 & 8 \end{bmatrix}$

Forme a matriz $M = (A, I)$ e reduza M para a forma escada:

$$M = \begin{bmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 2 & 1 & 3 & 0 & 1 & 0 \\ 4 & 1 & 8 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & -1 & 2 & 1 & 0 \\ 0 & 1 & 0 & -4 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 0 \\ 0 & 0 & -1 & -6 & 1 & 1 \end{bmatrix}$$

Na forma escada, a metade esquerda de M está na forma triangular; logo, S é inversível. Reduza ainda mais as linhas de M para a forma canônica de linha.

$$M \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & -1 & 0 & 4 & 0 & -1 \\ 0 & 0 & 1 & 6 & 1 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 11 & 2 & 2 \\ 0 & 1 & 0 & -4 & 0 & 1 \\ 0 & 0 & 1 & 6 & 1 & 1 \end{array}\right]$$

A matriz identidade é a metade esquerda da matriz final, logo, a metade direita é A^{-1}. Em outras palavras,

$$A^{-1} = \begin{bmatrix} -11 & 2 & 2 \\ 4 & 0 & 1 \\ 6 & 1 & 1 \end{bmatrix}$$

A.11 MATRIZES BOOLEANAS (ZERO-UM)

Os *dígitos binários* ou *bits* são os símbolos 0 e 1. Considere as seguintes operações nesses dígitos.

+	0	1
0	0	1
1	1	1

×	0	1
0	0	0
1	0	1

Vendo esses bits como valores lógicos (0 representando FALSO e 1 representando VERDADEIRO), as operações acima correspondem, respectivamente, às operações lógicas de OR (∨) e AND (∧); isto é,

∨	F	V
F	F	V
V	V	V

∧	F	V
F	F	F
V	F	V

(As operações acima em 0 e 1 são chamadas de *operações Booleanas*, uma vez que elas também correspondem às operações da álgebra Booleana discutidas no Capítulo 15.)

Agora considere que $A = [a_{ij}]$ é uma matriz cujas entradas são os bits 0 e 1, sujeitos às operações Booleanas acima. Então A é chamada de *matriz Booleana*. O *produto Booleano* de duas matrizes dessa classificação é o produto usual, exceto pelo fato de que agora usamos operações Booleanas de adição e multiplicação. Por exemplo, se

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ e } B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \text{ então } AB = \begin{bmatrix} 0+0 & 1+1 \\ 0+0 & 1+0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

É fácil mostrar que, se A e B são matrizes Booleanas, então o produto Booleano AB pode ser obtido encontrando o produto usual de A e B e substituindo qualquer dígito diferente de zero por 1.

Problemas Resolvidos

Vetores

A.1 Seja $u = (2, -7, 1)$, $v = (-3, 0, 4)$ e $w = (0, 5, -8)$. Encontre: (*a*) $3u - 4v$; (*b*) $2u + 3v - 5w$.

Realize, primeiro, a multiplicação escalar e, em seguida, a adição vetorial.

(*a*) $3u - 4v = 3(2, -7, 1) - 4(-3, 0, 4) = (6, -21, 3) + (12, 0, -16) = (18, -21, -13)$.

(*b*) $2u + 3v - 6w = 2(2, -7, 1) + 3(-3, 0, 4) - 5(0, 5, -8) = (4, -14, 2) + (-9, 0, 12) + (0, -25, 40)$
$= (-5, -39, 54)$.

A.2 Para o vetor u, v e w no Problema A.1, encontre: (*a*) $u \cdot v$; (*b*) $u \cdot w$; (*c*) $v \cdot w$.

Multiplique as componentes correspondentes e então some

(*a*) $u \cdot v = 2(-3) - 7(0) + 1(4) = -6 + 0 + 4 = -2$.

(*b*) $u \cdot w = 2(0) - 7(5) + 1(-8) = 0 - 35 - 8 = -43$

(*c*) $v \cdot w = -3(0) + 0(5) + 4(-8) = 0 + 0 - 32 = -32$.

A.3 Encontre $\|u\|$ onde: (*a*) $u = (3, -12, -4)$; (*b*) $u = (2, -3, 8, -7)$.

Primeiro, encontre $\|u\|^2 = u \cdot u$ ao elevar as componentes ao quadrado e somar. Então $\|u\| = \sqrt{u \cdot u}$

(*a*) $\|u\|^2 = (3)^2 + (-12)^2 + (-4)^2 = 9 + 144 + 16 = 169$. Logo, $\|u\| = \sqrt{169} = 13$.

(*b*) $\|u\|^2 = 4 + 9 + 64 + 49 = 126$. Logo, $\|u\| = \sqrt{126}$.

A.4 Encontre x e y se $x(1, 1) + y(2, -1) = (1, 4)$

Primeiro, multiplique os escalares x e y e então some:

$$x(1, 1) + y(2, -1) = (x, x) + (2y, -y) = (x + 2y, x - y) = (1, 4)$$

Dois vetores são iguais apenas quando suas componentes correspondentes são iguais, logo, considere as componentes correspondentes iguais umas às outras, para obter $x + 2y = 1$ e $x - y = 4$. Finalmente, resolva o sistema de equações para obter $x = 3$ e $y = -1$

A.5 Suponha que $u = \begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix}$, $v = \begin{bmatrix} -1 \\ 5 \\ 2 \end{bmatrix}$ e $w = \begin{bmatrix} 3 \\ -1 \\ -2 \end{bmatrix}$. Encontre: (*a*) $5u - 2v$; (*b*) $-2u + 4v - 3w$.

(*a*) $5u - 2v = 5\begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix} - 2\begin{bmatrix} -1 \\ 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 25 \\ 15 \\ -20 \end{bmatrix} + \begin{bmatrix} 2 \\ -10 \\ -4 \end{bmatrix} = \begin{bmatrix} 27 \\ 5 \\ -24 \end{bmatrix}$

(*b*) $-2u + 4v - 3w = \begin{bmatrix} -10 \\ -6 \\ 8 \end{bmatrix} + \begin{bmatrix} -4 \\ 20 \\ 8 \end{bmatrix} + \begin{bmatrix} -9 \\ 3 \\ 6 \end{bmatrix} = \begin{bmatrix} -23 \\ 17 \\ 22 \end{bmatrix}$

Adição de matrizes e multiplicação escalar

A.6 Encontre $2A - 3B$, onde $A = \begin{bmatrix} 1 & -2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ e $B = \begin{bmatrix} 3 & 0 & 2 \\ -7 & 1 & 8 \end{bmatrix}$

Primeiro, realize as multiplicações escalares e então uma adição de matrizes:

$$2A - 3B = \begin{bmatrix} 2 & -4 & 6 \\ 8 & 10 & 12 \end{bmatrix} + \begin{bmatrix} -9 & 0 & -6 \\ 21 & -3 & -24 \end{bmatrix} = \begin{bmatrix} -7 & -4 & 0 \\ 29 & 7 & -36 \end{bmatrix}$$

(Note que multiplicamos B por -3 e então somamos, em vez de multiplicar B por 3 e subtrair. Isso geralmente evita erros.)

A.7 Encontre x, y, z e t, onde $3\begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} x & 6 \\ -1 & 2t \end{bmatrix} + \begin{bmatrix} 4 & x + y \\ z + t & 3 \end{bmatrix}$

Primeiro, escreva cada lado como uma única matriz

$$\begin{bmatrix} 3x & 3y \\ 3z & 3t \end{bmatrix} = \begin{bmatrix} x + 4 & x + y + 6 \\ z + t - 1 & 2t + 3 \end{bmatrix}$$

Considere as entradas correspondentes como iguais umas às outras para obter o sistema de quatro equações,

$$3x = x + 4, \quad 3y = x + y + 6, \quad 3z = z + t - 1, \quad 3t = 2t + 3$$

ou

$$2x = 4, \quad 2y = 6 + x, \quad 2z = t - 1, \quad t = 3$$

A solução é $x = 2$, $y = 4$, $z = 1$, $t = 3$.

A.8 **Demonstre o Teorema A.1(v): $k(A + B) = kA + kB$**

Sejam $A = [a_{ij}]$ e $B = [b_{ij}]$. Então a entrada ij de $A + B$ é $a_{ij} + b_{ij}$. Logo, $k(a_{ij} + b_{ij})$ é a entrada ij de $k(A + B)$. Por outro lado, as entradas ij de kA e kB são ka_{ij} e kb_{ij}, respectivamente. Então, $ka_{ij} + kb_{ij}$ é a entrada ij de $kA + kB$. Contudo, para escalares, $k(a_{ij} + b_{ij}) = ka_{ij} + kb_{ij}$. Portanto, $k(A + B)$ e $kA + kB$ possuem as mesmas entradas ij. Logo, $k(A + B) = kA + kB$.

Multiplicação de matrizes e transposta

A.9 **Calcule:** (*a*) $[3, -2, 5]\begin{bmatrix} 6 \\ 1 \\ -4 \end{bmatrix}$; (*b*) $[2, -1, 7, 4]\begin{bmatrix} 5 \\ -3 \\ 6 \\ 9 \end{bmatrix}$

Multiplique as entradas correspondentes e então some:

(*a*) $[3, -2, 5]\begin{bmatrix} 6 \\ 1 \\ -4 \end{bmatrix} = 18 - 2 - 20 = -4$. (*b*) $[2, -1, 7, 4]\begin{bmatrix} 5 \\ 3 \\ -6 \\ 9 \end{bmatrix} = 10 + 3 - 42 + 36 = 7$

A.10 **Considere que** $A = \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ **e** $B = \begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix}$. **Encontre:** (*a*) AB; (*b*) BA.

(*a*) Uma vez que A é 2×2 e B é 2×3, o produto AB é definido como uma matriz 2×3. Para obter a primeira linha de AB, multiplique a primeira linha $[1, 3]$ de A pelas colunas $\begin{bmatrix} 2 \\ 3 \end{bmatrix}$, $\begin{bmatrix} 0 \\ -2 \end{bmatrix}$, $\begin{bmatrix} -4 \\ 6 \end{bmatrix}$ de B, respectivamente:

$$\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 1(2) + 3(3) & 1(0) + 3(-2) & 1(-4) + 3(6) \end{bmatrix}$$
$$= \begin{bmatrix} 2 + 9 & 0 - 6 & -4 + 18 \end{bmatrix} = \begin{bmatrix} 11 & -6 & 14 \end{bmatrix}$$

Para obter as entradas na segunda linha de AB, multiplique a segunda linha $[2, -1]$ de A pelas colunas de B, respectivamente:

$$\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 11 & -6 & 14 \\ 4 - 3 & 0 + 2 & -8 - 6 \end{bmatrix}$$

Logo,

$$AB = \begin{bmatrix} 11 & -6 & 14 \\ 1 & 2 & -14 \end{bmatrix}$$

(*b*) Note que B é 2×3 e A é 2×2. Uma vez que os números internos, 3 e 2, não são iguais, o produto BA não é definido.

A.11 **Encontre a transposta de cada matriz:**

$$A = \begin{bmatrix} 1 & -2 & 3 \\ 7 & 8 & -9 \end{bmatrix}; \quad B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}; \quad C = [1, -3, 5, -7]; \quad D = \begin{bmatrix} 2 \\ -4 \\ 6 \end{bmatrix}$$

Reescreva as linhas de cada matriz como colunas para obter a transposta dessas matrizes.

$$A^T = \begin{bmatrix} 1 & 7 \\ -2 & 8 \\ 3 & -9 \end{bmatrix}, \quad B^T = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}, \quad C^T = \begin{bmatrix} 1 \\ -3 \\ 5 \\ -7 \end{bmatrix}, \quad D^T = [2, -4, 6]$$

(Note que $B^T = B$; tal matriz é chamada de *simétrica*. Note também que a transposta do vetor linha C é um vetor coluna, e a transposta do vetor coluna D é um vetor linha.)

A.12 Demonstre o Teorema A.2(i): $A(BC) = A(BC)$.

Sejam $A = [a_{ij}]$, $B = [b_{jk}]$ e $C = [c_{kl}]$. Além disso, considere que $AB = S = [s_{ik}]$ e $BC = T = [t_{jl}]$.

Então

$$s_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{im}b_{mk} = \sum_{j=1}^{m} a_{ij}b_{jk}$$

$$t_{jl} = b_{j1}c_{1l} + b_{j2}c_{2l} + \cdots + b_{jn}c_{nl} = \sum_{k=1}^{n} b_{jk}c_{kl}$$

Agora, multiplicando S por C, isto é, (AB) por C, o elemento na i-ésima linha e l-ésima coluna da matriz $(AB)C$ é

$$s_{i1}c_{1l} + s_{i2}c_{2l} + \cdots + s_{in}c_{nl} = \sum_{k=1}^{n} s_{ik}c_{kl} = \sum_{k=1}^{n}\sum_{j=1}^{m}(a_{ij}b_{jk})c_{kl}$$

Por outro lado, multiplicando A por T, isto é, A por BC, o elemento na i-ésima linha e l-ésima coluna da matriz $A(BC)$ é

$$a_{i1}t_{1l} + a_{i2}t_{2l} + \cdots + a_{im}t_{ml} = \sum_{j=1}^{m} a_{ij}t_{jl} = \sum_{j=1}^{m}\sum_{k=1}^{n} a_{ij}(b_{jk}c_{kl})$$

Uma vez que as somas acima são iguais, o teorema está demonstrado.

Matrizes quadradas, determinantes, inversas

A.13 Encontre a diagonal e o traço de cada matriz:

$$(a)\ A = \begin{bmatrix} 1 & 3 & 6 \\ 2 & -5 & 8 \\ 4 & -2 & 7 \end{bmatrix};\quad (b)\ B = \begin{bmatrix} t-2 & 3 \\ -4 & t+5 \end{bmatrix};\quad (c)\ C = \begin{bmatrix} 1 & 2 & -3 \\ 4 & 5 & 6 \end{bmatrix}$$

(*a*) A diagonal consiste nos elementos a_{11}, a_{22} e a_{33}, isto é, os escalares 1, -5 e 7. O traço é a soma dos elementos da diagonal, logo, $\text{tr}(A) = 1 - 5 + 7 = 3$.

(*b*) A diagonal consiste no par $\{t-2, t+5\}$. Logo, $\text{tr}(B) = t - 2 + t + 5 = 2t + 3$.

(*c*) A diagonal e o traço são definidos apenas para matrizes quadradas.

A.14 Seja $A = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}$. Encontre: (*a*) A^2; (*b*) A^3, (*c*) $f(A)$ onde $f(x) = 2x^3 - 4x + 5$, (*d*) $g(A)$ onde $g(x) = x^2 + 2x - 11$.

$$(a)\ A^2 = AA = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} = \begin{bmatrix} 1+8 & 2-6 \\ 4-12 & 8+9 \end{bmatrix} = \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix}$$

$$(b)\ A^3 = AA^2 = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}\begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} = \begin{bmatrix} 9-16 & -4+34 \\ 36+24 & -16-51 \end{bmatrix} = \begin{bmatrix} -7 & 30 \\ 60 & -67 \end{bmatrix}$$

(*c*) Calcule $f(A)$ substituindo, em primeiro lugar, A por x e $5I$ pelo termo constante em $f(x) = 2x^3 - 4x + 5$

$$f(A) = 2A^3 - 4A + 5I = 2\begin{bmatrix} -7 & 30 \\ 60 & -67 \end{bmatrix} - 4\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Então multiplique cada matriz pelo seu respectivo escalar:

$$f(A) = \begin{bmatrix} -14 & 60 \\ 120 & -134 \end{bmatrix} + \begin{bmatrix} -4 & -8 \\ -16 & 12 \end{bmatrix} + \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

Por último, some os elementos correspondentes nas matrizes:

$$f(A) = \begin{bmatrix} -14-4+5 & 60-8+0 \\ 120-16+0 & -134+12+5 \end{bmatrix} = \begin{bmatrix} -13 & 52 \\ 104 & -117 \end{bmatrix}$$

(d) Calcule $g(A)$ substituindo, em primeiro lugar, A por x e $11I$ pelo termo constante 11 em $g(x) = x^2 + 2x - 11$

$$g(A) = A^2 + 2A - 11I = \begin{bmatrix} 9 & 4 \\ 8 & 17 \end{bmatrix} + 2\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} - 11\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 4 \\ 8 & 17 \end{bmatrix} + \begin{bmatrix} 2 & 4 \\ 8 & -6 \end{bmatrix} + \begin{bmatrix} -11 & 0 \\ 0 & -11 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

(Uma vez que $g(A) = 0$, a matriz A é um zero do polinômio $g(x)$.)

A.15 Calcule cada determinante: (a) $\begin{vmatrix} 4 & 5 \\ -3 & -2 \end{vmatrix}$; ($b$) $\begin{vmatrix} a-b & b \\ b & a+b \end{vmatrix}$

(a) $\begin{vmatrix} 4 & 5 \\ -3 & -2 \end{vmatrix} = 4(-2) - (-3)(5) = -8 + 15 = 7.$

(b) $\begin{vmatrix} a-b & b \\ b & a+b \end{vmatrix} = (a-b)(a+b) - b^2 = a^2 - b^2 - b^2 = a^2 - 2b^2$

A.16 Encontre o determinante de cada matriz.

(a) $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & -2 & 3 \\ 0 & 5 & -1 \end{bmatrix}$; ($b$) $B = \begin{bmatrix} 4 & -1 & -2 \\ 0 & 2 & -3 \\ 5 & 2 & 1 \end{bmatrix}$, ($c$) $C = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 3 \\ 1 & 2 & 5 \end{bmatrix}$

(Sugestão: Use o diagrama na Fig. A.3 (b)):

(a) $|A| = 2 + 0 + 60 - 0 - 15 + 8 = 55$

(b) $|B| = 8 + 15 + 0 + 20 + 24 + 0 = 67$

(c) $|C| = 20 - 9 - 8 + 8 - 12 + 15 = 14$

A.17 Encontre a inversa de (a) $A = \begin{bmatrix} 5 & 3 \\ 4 & 2 \end{bmatrix}$; ($b$) $B = \begin{bmatrix} -2 & 6 \\ 3 & 9 \end{bmatrix}$

Use a fórmula na Seção A.9.

(a) Encontre, primeiro, $|A| = 5(2) - 3(4) = 10 - 12 = -2$. Em seguida, permute os elementos diagonais, use os negativos dos elementos não diagonais e multiplique por $1/|A|$:

$$A^{-1} = -\frac{1}{2}\begin{bmatrix} 2 & -3 \\ -4 & 5 \end{bmatrix} = \begin{bmatrix} -1 & \frac{3}{2} \\ 2 & -\frac{5}{2} \end{bmatrix}$$

(b) Primeiro, encontre $|B| = -2(-9) - 6(3) = 18 - 18 = 0$. Uma vez que $|B| = 0$, B não possui inversa.

A.18 Encontre a inversa de: (a) $A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -3 & 6 \\ 1 & 1 & 7 \end{bmatrix}$; ($b$) $B = \begin{bmatrix} 1 & 3 & -4 \\ 1 & 5 & -1 \\ 3 & 13 & -6 \end{bmatrix}$.

(a) Forme a matriz $M = [A, I]$ e reduza as linhas de M para a forma escada:

$$M = \left[\begin{array}{ccc|ccc} 1 & 2 & 2 & 1 & 0 & 0 \\ 2 & 3 & 6 & 0 & 1 & 0 \\ 1 & 1 & 7 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 3 & 5 & -1 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 0 & -1 & 5 & -3 & 1 \end{array}\right]$$

Na forma escada, a metade esquerda de M está na forma triangular, uma vez que A possui uma inversa. Reduza novamente M para a forma canônica de linhas.

$$M = \left[\begin{array}{ccc|ccc} 1 & 2 & 0 & 11 & 6 & 2 \\ 0 & 1 & 0 & 8 & 5 & 2 \\ 0 & 0 & 1 & 5 & 3 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 27 & 16 & 6 \\ 0 & 1 & 0 & 8 & 5 & 2 \\ 0 & 0 & 1 & 5 & 3 & 1 \end{array}\right]$$

A matriz final possui a forma $[I, A^{-1}]$, isto é, A^{-1} é a metade direita da última matriz. Logo,

$$A^{-1} = \begin{bmatrix} 27 & -16 & 6 \\ 8 & -5 & 2 \\ -5 & 3 & -1 \end{bmatrix}$$

(*b*) Forme a matriz $M = [B, I]$ e reduza as linhas de M para a forma escada:

$$M \begin{bmatrix} 1 & 3 & 4 & 1 & 0 & 0 \\ 1 & 5 & -1 & 0 & 1 & 0 \\ 3 & 13 & -6 & 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 3 & 4 & 1 & 0 & 0 \\ 0 & 2 & 3 & 1 & 1 & 0 \\ 0 & 4 & 6 & -3 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & 4 & 1 & 0 & 0 \\ 0 & 2 & 3 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -2 & 1 \end{bmatrix}$$

Na forma escada, M possui uma linha nula na sua metade esquerda, isto é, B agora é redutível à forma triangular Em conformidade, B não possui inverso.

Matrizes escada, redução de linhas, eliminação Gaussiana

A.19 Permute as linhas em cada matriz para obter uma matriz escada.

$$(a) \begin{bmatrix} 0 & 1 & -3 & 4 & 6 \\ 4 & 0 & 2 & 5 & -3 \\ 0 & 0 & 7 & -2 & 8 \end{bmatrix}; \quad (b) \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 5 & -4 & 7 \end{bmatrix}; \quad (c) \begin{bmatrix} 0 & 2 & 2 & 2 & 2 \\ 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

(*a*) Permute a primeira e a segunda linha.

(*b*) Arraste a linha nula para a parte inferior da matriz.

(*c*) Nenhum número de permutação de linhas poderia produzir uma matriz escada.

A.20 Reduza as linhas da matriz $A = \begin{bmatrix} 1 & 2 & -3 & 0 \\ 2 & 4 & -2 & 2 \\ 3 & 6 & -4 & 3 \end{bmatrix}$ para a forma escada.

Use a_{11} como um pivô para obter zeros abaixo de a_{11}, isto é, aplique as operações de linha "Some $2R_1$ a R_2" e "Some $-3R_1$ a R_3;" então use a_{23} 4 como um pivô para obter um zero abaixo de a_{23}, isto é, aplicando a operação de linha "Some $5R_2$ a $4R_3$." Essas operações implicam o que segue, onde a última matriz está na forma escada.

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 5 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

A.21 Quais das seguintes matrizes estão na forma canônica de linhas?

$$\begin{bmatrix} 1 & 2 & -3 & 0 & 1 \\ 0 & 0 & 5 & 2 & 4 \\ 0 & 0 & 0 & 7 & 3 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 7 & 5 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 5 & 0 & 2 \\ 0 & 1 & 2 & 0 & 4 \\ 0 & 0 & 0 & 1 & 7 \end{bmatrix}$$

A primeira matriz não está na forma canônica de linhas, uma vez que, por exemplo, duas entradas principais diferentes de zero são 5 e 7, não 1 Além disso, existem entradas diferentes de zero acima das entradas principais diferentes de zero 5 e 7. A segunda e a terceira matriz estão na forma canônica de linhas.

A.22 Reduza a matriz $A = \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 1 & 1 & 4 & 1 & 3 \\ 2 & 5 & 9 & -2 & 8 \end{bmatrix}$ à forma canônica de linhas

Primeiro, reduza A à forma escada, aplicando as operações "Some R_1 a R_2", "Some $-2R_1$ a R_3" e, então, "Some $-3R_2$ a R_3". Essas operações implicam

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & 2 & 1 \\ 0 & 9 & 3 & 4 & 4 \end{bmatrix} \quad \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & 2 & 1 \\ 0 & 0 & 0 & 2 & 1 \end{bmatrix}$$

Agora use substituição retroativa na matriz escada para obter a forma canônica de linha de A. Especificamente, multiplique R_3 por $\frac{1}{2}$ para obter o pivô $a_{34} = 1$, então aplique as operações "Some $2R_3$ a R_2" e "Some $-R_3$ a R_1". Essas operações implicam

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 3 & 0 & \frac{3}{2} \\ 0 & 3 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix}$$

Agora multiplique R_2 por $\frac{1}{3}$, fazendo o pivô $a_{22} = 1$ e aplique a operação "Some $2R_2$ a R_1". Obtemos

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 0 & \frac{3}{2} \\ 0 & 1 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \frac{11}{3} & 0 & \frac{17}{6} \\ 0 & 1 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix}$$

Uma vez que $a_{11} = 1$, a última matriz é a forma canônica de linha de A que foi pedida.

A.23 Resolva cada sistema, usando sua matriz aumentada M:

$$(a)\quad \begin{aligned} x + y - 2z + 4t &= 5 \\ 2x + 2y - 3z + t &= 4 \\ 3x + 3y - 4z - 2t &= 3 \end{aligned} \qquad (b)\quad \begin{aligned} x - 2y + 4z &= 2 \\ 2x - 3y + 5z &= 3 \\ 3x - 4y + 6z &= 7 \end{aligned}$$

(a) Reduza sua matriz aumentada M para a forma escada e, então, para a forma canônica de linhas:

$$M = \begin{bmatrix} 1 & 1 & -2 & 4 & 5 \\ 2 & 2 & -3 & 1 & 4 \\ 3 & 3 & -4 & -2 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & -2 & 4 & 5 \\ 0 & 0 & 1 & -7 & -6 \\ 0 & 0 & 2 & -14 & -12 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & -10 & -7 \\ 0 & 0 & 1 & -7 & -6 \end{bmatrix}$$

(A terceira linha da segunda matriz é deletada, uma vez que ela é um múltiplo da segunda linha, e resultará em uma linha nula.)

Escreva o sistema correspondente à forma canônica de linha de M e então transfira as variáveis livres ao outro lado para obter a forma de variável livre da solução

$$\begin{aligned} x + y - 10t &= -7 \\ z - 7t &= -6 \end{aligned} \quad \text{e, então,} \quad \begin{aligned} x &= -7 - y + 10t \\ z &= -6 + 7t \end{aligned}$$

Aqui, x e z são variáveis básicas, e y e t são as variáveis livres.

A forma *paramétrica* da solução pode ser obtida ao fixar as variáveis livres iguais aos *parâmetros*, digamos $y = a$ e $t = b$. Esse processo implica $x = -7 - a + 10b$, $y = a$, $z = -6 + 7b$, $t = b$ ou $u = (-7 - a + 10b, a, -6 + 7b, b)$ (que é outra forma da solução).

Uma *solução particular* pode ser obtida associando quaisquer valores às variáveis livres (ou parâmetros) e resolvendo para as variáveis básicas, usando qualquer forma da solução geral. Por exemplo, fixar $y = 2$ e $t = 3$, obtemos $x = 21$ e $z = 15$. Logo, a solução a seguir é uma solução particular do sistema:

$$x = 21, \quad y = 2, \quad z = 15, \quad t = 3 \quad \text{ou} \quad u = (21, 2, 15, 3)$$

(b) Primeiro, reduza as linhas da matriz aumentada M para a forma escada.

$$M = \begin{bmatrix} 1 & -2 & 4 & 2 \\ 2 & -3 & 5 & 3 \\ 3 & -4 & 6 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 4 & 2 \\ 0 & 1 & -3 & -1 \\ 0 & 2 & -6 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 4 & 2 \\ 0 & 1 & -3 & -1 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

Na forma escada, a terceira linha corresponde à equação reduzida $0x + 0y + 0z = 3$.

Logo, o sistema não possui solução. (Note que a forma escada indica se o sistema possui solução ou não.)

Problemas variados

A.24 Sejam $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ matrizes Booleanas,

Encontre os produtos Booleanos AB, BA e A^2,

Encontre o produto usual da matriz e, então, substitua 1 por qualquer escalar diferente de zero. Logo:

$$AB = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix};\ BA = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ A^2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

A.25 Seja $A = \begin{bmatrix} 1 & 3 \\ 4 & -3 \end{bmatrix}$ (*a*) Encontre um vetor coluna diferente de zero $u = \begin{bmatrix} x \\ y \end{bmatrix}$ tal que $Au = 3u$. (*b*) Descreva tais vetores.

(*a*) Primeiro organize a equação da matriz $Au = 3u$ e, então, escreva cada lado na forma de uma matriz singular (vetor coluna):

$$\begin{bmatrix} 1 & 3 \\ 4 & -3 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = 3\begin{bmatrix} x \\ y \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} x + 3y \\ 4x - 3y \end{bmatrix} = \begin{bmatrix} 3x \\ 3y \end{bmatrix}$$

Fixe elementos correspondentes iguais entre si, para obter um sistema de equações, e reduza o sistema à forma escada.

$$\begin{aligned} x + 3y &= 3x \\ 4x - 3y &= 3y \end{aligned} \quad \text{ou} \quad \begin{aligned} 2x - 3y &= 0 \\ 4x - 6y &= 0 \end{aligned} \quad \text{para} \quad \begin{aligned} 2x - 3y &= 0 \\ 0 &= 0 \end{aligned} \quad \text{ou} \quad 2x - 3y = 0$$

O sistema se reduz a uma equação linear (não degenerada) com duas incógnitas e, portanto, possui um número infinito de soluções. Para obter uma solução diferente de zero, fixe $y = 2$ e $x = 3$. Logo, $u = [3, 2]^T$ é uma solução diferente de zero, como pedido.

(*b*) Para encontrar a solução geral, fixe $y = a$, onde a é um parâmetro. Substitua $y = a$ por $2x - 3y = 0$ para obter $x = 3a/2$. Logo, $u = [3a/2, a]^T$ representa todas as soluções. Uma forma alternativa pode ser $y = 2b$, de modo que $v = [3b, 2b]$ represente todas as soluções.

Problemas Complementares

Vetores

A.26 Sejam $u = (2, -1, 0, -3)$, $v = (1, -1, -1, 3)$, $w = (1, 3, -2, 2)$. Encontre: (a) $2u - 3v$; (b) $5u - 3v - 4w$; (c) $-u + 2v - 2w$; (d) $u \cdot v$, $u \cdot w$, $v \cdot w$, (e) $\|u\|$, $\|v\|$, $\|w\|$

A.27 Sejam $u = \begin{bmatrix} 1 \\ 3 \\ -4 \end{bmatrix}$, $v = \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix}$, $w = \begin{bmatrix} 3 \\ -2 \\ 6 \end{bmatrix}$. Encontre (a) $5u - 3v$; (b) $2u + 4v - 6w$. (c) $u \cdot v$, $u \cdot w$, $v \cdot w$; (d) $\|u\|$, $\|v\|$, $\|w\|$.

A.28 Sejam x e y. Encontre: (a) $x(2, 5) + y(4, -3) = (8, 33)$; (b) $x(1, 4) + y(2, -5) = (7, 2)$.

Operações de matrizes

A.29 Seja $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 5 & 0 \\ 6 & 7 \end{bmatrix}$, $C = \begin{bmatrix} 1 & -3 & 4 \\ 2 & 6 & 5 \end{bmatrix}$, $D = \begin{bmatrix} 3 & 7 & -1 \\ 4 & 8 & 9 \end{bmatrix}$. Encontre

(a) $5A - 2B$ e $2C - 3D$; (c) AC e AD; (e) A^T e C^T,

(b) AB e BA; (d) BC e BD; (f) A^2, B^2, C^2.

A.30 Seja $A = \begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 4 & 0 & -3 \\ 1 & 2 & 3 \end{bmatrix}$, $C = \begin{bmatrix} 2 & -3 & 0 & 1 \\ 5 & 1 & 4 & 2 \\ -1 & 0 & 0 & 3 \end{bmatrix}$, $D = \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix}$

Encontre: (a) $3A - 4B$; (b) AB, AC, AD; (c) BC, BD, CD; (d) A^T e A^TB

A.31 Seja $A = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}$. Encontre uma matriz B 2×3 com entradas distintas, tal que $AB = 0$.

Matrizes quadradas

A.32 Encontre a diagonal e o traço de (a) $A = \begin{bmatrix} 2 & -7 & 8 \\ 3 & -6 & 5 \\ 4 & 0 & -1 \end{bmatrix}$, (b) $B = \begin{bmatrix} 1 & 2 & -9 \\ -3 & 2 & 8 \\ 5 & -6 & -1 \end{bmatrix}$

A.33 Seja $A = \begin{bmatrix} 2 & -5 \\ 3 & 1 \end{bmatrix}$. Encontre: (a) A^2 e A^3; (b) $f(A)$ onde $f(x) = x^3 - 2x^2 - 5$.

A.34 Seja $B = \begin{bmatrix} 4 & -2 \\ 1 & -6 \end{bmatrix}$. Encontre: (a) B^2 e B^3; (b) $f(B)$ onde $f(x) = x^2 + 2x - 22$.

A.35 Seja $A = \begin{bmatrix} 6 & 4 \\ 3 & 2 \end{bmatrix}$. Encontre um vetor diferente de zero $u = \begin{bmatrix} x \\ y \end{bmatrix}$ tal que $Au = 4u$.

Determinantes e inversas

A.36 Encontre cada determinante (a) $\begin{vmatrix} 2 & 5 \\ 4 & 1 \end{vmatrix}$; (b) $\begin{vmatrix} 6 & 1 \\ 3 & 2 \end{vmatrix}$; (c) $\begin{vmatrix} -2 & 8 \\ 5 & 2 \end{vmatrix}$, (d) $\begin{vmatrix} a-b & a \\ a & a+b \end{vmatrix}$

A.37 Calcule o determinante de cada matriz no Problema A.32.

A.38 Encontre a inversa de: (a) $A = \begin{bmatrix} 7 & 4 \\ 5 & 3 \end{bmatrix}$; (b) $B = \begin{bmatrix} 5 & 2 \\ 6 & 3 \end{bmatrix}$, (c) $C = \begin{bmatrix} 4 & 6 \\ 2 & 3 \end{bmatrix}$

A.39 Encontre a inversa de cada matriz (se existir):

$$A = \begin{bmatrix} 1 & 2 & -4 \\ 1 & -1 & 5 \\ 2 & 7 & -3 \end{bmatrix}; \quad B = \begin{bmatrix} 1 & -1 & 1 \\ 0 & 2 & 2 \\ 1 & 3 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 1 \\ 5 & 12 & 1 \end{bmatrix}$$

Matrizes escada, reduções de linha, eliminação Gaussiana

A.40 Reduza A para a forma escada e, então, para a forma canônica de linhas, onde:

$$\text{(a)}\ A = \begin{bmatrix} 1 & 2 & -1 & 2 & 1 \\ 2 & 4 & 1 & -2 & 3 \\ 3 & 6 & 2 & -6 & 5 \end{bmatrix}; \quad \text{(b)}\ A = \begin{bmatrix} 2 & 3 & -2 & 5 & 1 \\ 3 & -1 & 2 & 0 & 4 \\ 4 & -5 & 6 & -5 & 7 \end{bmatrix}.$$

A.41 Usando apenas 0's e 1's, liste todas as matrizes 2×2 na forma escada.

A.42 Usando apenas 0's e 1's, encontre o número de matrizes 2×3 na forma canônica de linha.

A.43 Resolva cada sistema

$$\text{(a)}\ \begin{aligned} x + 2y - 4z &= 3 \\ 2x + 6y - 5z &= 2 \\ 3x + 11y - 4z &= 12 \end{aligned} \qquad \text{(b)}\ \begin{aligned} x + 2y - 4z &= 3 \\ 2x + 6y - 5z &= 10 \\ 3x + 10y - 6z &= 14 \end{aligned}$$

A.44 Resolva cada sistema

$$\text{(a)}\ \begin{aligned} x - 3y + 2z - t &= 2 \\ 3x - 9y + 7z - t &= 7 \\ 2x - 6y + 7z + 4t &= 7 \end{aligned} \qquad \text{(b)}\ \begin{aligned} x + 2y + 3z &= 7 \\ x + 3y + z &= 6 \\ 2x + 6y + 5z &= 15 \\ 3x + 10y + 7z &= 23 \end{aligned}$$

Problemas variados

A.45 Seja $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$. Encontre: (a) A^n, (b) A^{-1}, (c) uma matriz B tal que $B^2 = A$.

A.46 Matrizes A e B são consideradas comutativas se $AB = BA$. Encontre todas as matrizes $\begin{bmatrix} x & y \\ z & t \end{bmatrix}$ que comutam com $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

A.47 Sejam $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ matrizes Booleanas.

Encontre as matrizes Booleanas: (a) $A + B$; (b) AB; (c) BA; (d) A^2; (e) B^2.

Respostas dos Problemas Complementares

Notação: $M = [R_1, R_2, \ldots; R_n]$ denota uma matriz com linhas $R_1, \ldots, R_n$.

A.26 (a) (1, 1, 3, −15); (b) (3, −14, 11, −32); (c) (−2, −7, 2, 5); (d) −6, −7, 6; (e) $\sqrt{14}$, $\sqrt{12} = 2\sqrt{3}$, $\sqrt{18} = 3\sqrt{2}$.

A.27 (a) $[-1, 12, -35]^T$; (b) $[-8, 22, -24]^T$; (c) −15, −27, 34, (d) $\sqrt{26}$, $\sqrt{30}$, 7.

A.28 (a) $x = 6$, $y = -1$; (b) $x = 3$, $y = 2$.

A.29 (a) [5, 10; 27, 34], [7, 27, 11, 8, 36, 37], (b) [−7, 14, 39, −28], [5, 10; 15, −40], (c) [5, 9, −6, −5, −33, 32], [11, −9, 17; −7, 53, 39], (d) [5, −15, 20; 8, 60, −59], [15, 35, −5; 10, −98, 69], (e) [1, 3, 2, −4], [1, 2; −3, 6, 4, −5], (f) [7, −6; −9, 22], [25, 0; −72, 49], C^2 não é definido.

A.30 (a) [−13, −3, 18, 4, 17, 0]; (b) AB não é definido, [5, 2, 4, 5, 11, 3, 12, 18], [9; 9], (c) [11, 12, 0, −5, −15, 5, 8, 4], [−1, 9], CD não é definido, (d) [1, 0; −1, 3; 2, 4], [4, 0, −3; −7, −6, 12; 4, 8, 6]

A.31 [2, 4, 6; −1, −2, −3]

A.32 (a) [2, −6, −1], −5, (b) [1, 2, −1], 2

A.33 (a) [−11, −15; 9, −14], [−67, 40; −24, −59], (b) [−50, 70; 42, −36].

A.34 (a) [14, 4; −2, 34], [60, −52; 26, −200] (b) $f(B) = 0$.

A.35 $[2a; a]$, para qualquer a diferente de zero.

A.36 (a) −18; (b) −15; (c) 44, (d) $-b^2$.

A.37 (a) 323; (b) 48.

A.38 (a) [3, −4, −5, 7], (b) [1, −2/3; 2, −5/3], (c) Não é definido.

A.39 (a) [−16, −11, 3, 7/2, 5/2, 1/2, 5/2, 3/2, 1/2], (b) [1, 1/2, 0; −1/2, −1/2, 1/2; −1/2, −1, 1/2], (c) Não é definido.

A.40 (a) [1, 2, −1, 2, 1, 0, 0, 3, −6, 1; 0, 0, 0, −6, 1], [1, 2, 0, 0, 4/3, 0, 0, 1, 0, 0; 0, 0, 0, 1, −1/6], (b) [2, 3, −2, 5, 1, 0, 11, 10, 15, 5; 0, , 0], [1, 0, 4/11, 5/11, 13/11, 0, 1, −10/11, 15/11, −5/11; 0, . . . , 0]

A.41 [1, 1; 0, 1], [1, 1, 0, 0], [1, 0; 0, 0], [0, 1, 0, 0], [0, 0; 0, 0], [1, 0; 0, 1]

A.42 Existem 13.

A.43 (a) $x = 3$, $y = 1$, $z = 2$, (b) Não há solução.

A.44 (a) $x = 3y + 5t$, $z = 1 - 2t$, (b) $x = 2$, $y = 1$, $z = 1$

A.45 (a) $[1, 2n; 0, 1]$; (b) [1, −2, 0, 1]; (c) [1, 1, 0, 1].

A.46 $[a, b, 0, a]$.

A.47 (a) [110; 101; 111]; (b) [100; 111; 100]; (c) [010; 010; 101], (d) [101; 110; 010], (e) [100; 100; 111].

Sistemas Algébricos

B.1 INTRODUÇÃO

Este apêndice investiga alguns dos mais importantes sistemas algébricos na matemática semigrupos, grupos, anéis e corpos. Definimos também as noções de homomorfismo e de estrutura quociente. Começamos com a definição formal de uma operação e discutimos vários tipos de operações.

B.2 OPERAÇÕES

O leitor está familiarizado com as operações de adição e multiplicação de números, união e interseção de conjuntos, e a composição de funções. Essas operações são denotadas como se segue:

$$a+b=c, \quad a \cdot b=c, \quad A \cup B=C, \quad A \cap B=C, \quad g \circ f=h.$$

Em cada situação, um elemento (c, C ou h) é associado a um par original de elementos. Desenvolvemos maior precisão a essa noção.

Definição B.1: Seja S um conjunto não vazio. Uma *operação* em S é uma função $*$ de $S \times S$ em S. Em tal caso, em vez de $*(a, b)$, escrevemos normalmente

$$a * b \text{ ou, às vezes, } ab$$

O conjunto S e uma operação $*$ em S é denotada por $(S, *)$, ou apenas S, quando a operação é entendida.

Observação: Uma operação $*$ de $S \times S$ em S é, às vezes, chamada de *operação binária*. Uma operação *unária* é uma função de S em S. Por exemplo, o valor absoluto $|n|$ de um inteiro n é uma operação unária em **Z**, e o complemento A^c de um conjunto A é uma operação unária no conjunto potência $P(X)$ de um conjunto X. Uma operação *ternária* é uma função $S \times S \times S$ em S. De forma mais geral, uma função n-ária é uma função de $S \times S \times \cdots \times S$ (n fatores) em S. A menos que seja previamente observado, a palavra operação remeterá à operação binária. Assumiremos também que nosso conjunto básico S é não vazio.

Suponha que S é um conjunto finito. Então, uma operação $*$ em S pode ser apresentada por sua tabela de operação (multiplicação), onde a entrada na linha marcada por a e a coluna marcada por b é $a * b$.

Suponha que S é um conjunto com uma operação $*$, e suponha que A é um subconjunto de S. Então, A é dito *fechado sob* $*$ se $a * b$ pertence a A para quaisquer elementos a e b em A.

Exemplo B.1 Considere o conjunto **N** de inteiros positivos.

(a) Adição (+) e multiplicação (×) são operações em **N**. Contudo, subtração (−) e divisão (/) não são operações em **N**, uma vez que a diferença e o quociente de inteiros positivos não precisam ser inteiros positivos. Por exemplo, 2 − 9 e 7/3 não são inteiros positivos.

(b) Sejam A e B a notação, respectivamente, dos conjuntos de inteiros positivos pares e ímpares. Então, A é fechado sob adição e multiplicação, uma vez que a soma e o produto de quaisquer números pares resultam em outro número par. Por outro lado, B é fechado sob multiplicação, mas não adição, uma vez que, por exemplo, $3 + 5 = 8$ é par.

Exemplo B.2 Considere $S = \{a, b, c, d\}$. As tabelas na Fig. B-1 definem operações $*$ e em S. Note que $*$ pode ser definido pelas operações a seguir, onde x e y são quaisquer elementos de S:

$$x * y = x$$

*	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

(a)

	a	b		d
a	a	b	c	d
b	b	a	a	b
c	c	b	a	a
a	d	a	a	a

(b)

Figura B-1

A seguir, listamos algumas propriedades importantes de nossas operações.

Lei Associativa:

Uma operação $*$ em um conjunto S é dita *associativa*, ou satisfaz a *Lei Associativa*, se, para quaisquer elementos a, b e c em S, temos

$$(a * b) * c = a * (b * c)$$

Falando de forma geral, se uma operação não for associativa, então podem existir várias maneiras de formar um produto. Por exemplo, a seguir mostramos cinco maneiras de formar o produto $abcd$:

$$((ab)c)d, \quad (ab)(cd), \quad (a(bc))d, \quad a((bc)d), \quad a(b(cd))$$

Se a operação é associativa, então o teorema a seguir (demonstrado no Problema B.4) se aplica.

Teorema B.1: Suponha que $*$ é uma operação associativa em um conjunto S. Então, qualquer produto $a_1 * a_2 * \cdots * a_n$ não precisa de parênteses, isto é, todos os produtos possíveis são iguais.

Lei Comutativa:

Uma operação $*$ em um conjunto S é dita *comutativa*, ou satisfaz a *Lei Comutativa*, se, para quaisquer elementos a e b em S,

$$a * b = b * a$$

Exemplo B.3

(a) Considere o conjunto **Z** de inteiros. Adição e multiplicação de inteiros são associativas e comutativas. Por outro lado, subtração é não associativa. Por exemplo,

$$(8 - 4) - 3 = 1, \quad \text{mas} \quad 8 - (4 - 3) = 7$$

Além disso, subtração não é comutativa, uma vez que, por exemplo, $3 - 7 \neq 7 - 3$

(b) Considere a operação de multiplicação de matrizes no conjunto M de matrizes n-quadradas. É possível provar que multiplicação de matrizes é associativa. Por outro lado, multiplicação de matrizes não é comutativa. Por exemplo,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 15 & 10 \end{bmatrix}, \quad \text{mas} \quad \begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ -6 & -8 \end{bmatrix}$$

Elemento Identidade:

Considere uma operação $*$ em um conjunto S. Um elemento e em S é chamado de elemento *identidade* para $*$ se, para qualquer elemento a em S,

$$a * e = e * a = a$$

De forma mais geral, um elemento e é chamado de *identidade à esquerda* ou *identidade à direita*, dependendo se $e * a = a$ ou $a * e = a$, onde a é qualquer elemento de S. O seguinte teorema se aplica.

Teorema B.2: Suponha que e é uma identidade à esquerda e f é uma identidade à direita para uma operação em um conjunto S. Então $e = f$.

A demonstração é muito simples. Uma vez que e é uma identidade à esquerda, $ef = f$; mas, uma vez que f é uma identidade à direita, $ef = e$. Logo, $e = f$. Esse teorema nos diz, em particular, que um elemento identidade é único e que, se uma operação possui mais de um elemento identidade à esquerda, então ela não possui um elemento identidade à direita, e vice-versa.

Inversos:

Suponha que uma operação $*$ em um conjunto S possui um elemento identidade e. O *inverso* de um elemento a em S é um elemento b tal que

$$a * b = b * a = e$$

Se a operação for associativa, então o inverso de a, se existir, é único (Problema B.2). Observe que, se b é o inverso de a, então a é o inverso de b. Logo, o inverso é uma relação simétrica e podemos dizer que elementos a e b são inversos.

Notação: Se a operação em S é denotada por $a * b$, $a \times b$, $a \cdot b$ ou ab, então S é dito como sendo escrito *multiplicativamente* e o inverso de um elemento $a \in S$ é, usualmente, denotado por a^{-1}. Às vezes, quando S é comutativo, a operação é denotada por $+$ e, então, S é dito como sendo escrito *aditivamente*. Em tal caso, o elemento identidade é normalmente denotado por 0 e é chamado de elemento *zero*; o inverso é denotado por $-a$ e é chamado de *negativo* de a.

Exemplo B.4 Considere os números racionais **Q**. Sob adição, 0 é o elemento identidade, e -3 e 3 são inversos (aditivos), uma vez que

$$(-3) + 3 = 3 + (-3) = 0$$

Por outro lado, sob multiplicação, 1 é o elemento identidade e -3 e $-1/3$ são inversos (multiplicativos), uma vez que

$$(-3)(-1/3) = (-1/3)(-3) = 1$$

Note que 0 não possui inverso multiplicativo.

Leis de Cancelamento:

Uma operação $*$ em um conjunto S é dita satisfazendo a *Lei de Cancelamento à esquerda* ou a *Lei de Cancelamento à direita*, dependendo se,

$$a * b = a * c \text{ implica } b = c, \quad \text{ou} \quad b * a = c * a \text{ implica } b = c$$

Adição e subtração de inteiros em $\mathbf{Z}$ e multiplicação de inteiros diferentes de zero em $\mathbf{Z}$ satisfazem tanto a Lei de Cancelamento à esquerda quanto a da direita. Por outro lado, multiplicação de matrizes não satisfaz às Leis de Cancelamento. Por exemplo, suponha que

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & -3 \\ 1 & 5 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$

Então $AB = AC = D$, mas $B \neq C$.

B.3 SEMIGRUPOS

Seja S um conjunto não vazio com uma operação. Então S é chamado de *semigrupo* se a operação for associativa. Se a operação também possuir um elemento identidade, então S é chamado de *monoide*.

Exemplo B.5

(a) Considere os inteiros positivos $\mathbf{N}$. Então $(\mathbf{N}, +)$ e $(\mathbf{N}, \times)$ são semigrupos, uma vez que adição e multiplicação em $\mathbf{N}$ são operações associativas. Em particular, $(\mathbf{N}, \times)$ é um monoide, uma vez que ele possui o mesmo elemento identidade 1. Contudo, $(\mathbf{N}, +)$ não é um monoide, uma vez que adição em $\mathbf{N}$ não possui um elemento zero.

(b) Seja S um conjunto finito e $F(S)$ a coleção de todas as funções $f: S \to S$ sob a operação de composição de funções. Uma vez que a composição de funções é associativa, $F(S)$ é um semigupo. Na verdade, $F(S)$ é um monoide, uma vez que a função identidade é um elemento identidade para $F(S)$.

(c) Considere $S = \{a, b, c, d\}$. As tabelas de multiplicação na Fig. B-1 definem as operações $*$ e $\cdot$ em S. Note que $*$ pode ser definido pela fórmula $x * y = x$ para quaisquer x e y em S. Logo,

$$(x * y) * z = x * z = x \quad \text{e}\; x * (y * z) = x * y = x$$

Portanto, $*$ é associativa, logo, $(S, *)$ é um semigrupo. Por outro lado, $\cdot$ não é associativa, uma vez que, por exemplo,

$$(b \cdot c) \cdot c = a \cdot c = c, \quad \text{mas} \quad b \cdot (c \cdot c) = b \cdot a = b$$

Logo, $(S, \cdot)$ não é um semigrupo.

Semigrupo livre, monoide livre

Seja A um conjunto não vazio. Uma palavra w é uma sequência finita de seus elementos. Por exemplo, a seguir temos as palavras em $A = \{a, b, c\}$:

$$u = ababbbb = abab^4 \quad \text{e} \quad v = baccaaaa = bac^2a^4$$

(Escrevemos a^2 para aa, a^3 para aaa, e assim por diante.) O *comprimento* de uma palavra w, denotado por $l(w)$, é o número de elementos em w. Logo, $l(u) = 7$ e $l(v) = 8$.

A concatenação de palavras u e v em um conjunto A, escrita $u * v$ ou uv, é a palavra obtida pela escrita de elementos de u seguido dos elementos de v. Por exemplo,

$$uv = (abab^4)(bac^2a^4) = abab^5c^2a^4$$

Agora considere $F = F(A)$ como a notação para a coleção de todas as palavras em A sob a operação de concatenação. Claramente, para quaisquer palavras u, v e w, as palavras $(uv)w$ e $u(vw)$ são idênticas, elas simplesmente consistem nos elementos de u, v e w escritos um seguido do outro. Logo, F é um semigrupo; ele é chamado de *semigrupo livre* em A, e os elementos de A são chamados de *geradores* de F.

A sequência vazia, denotada por λ, é também considerada uma palavra em A. Contudo, não assumimos que λ pertence ao semigrupo livre $F = F(A)$. O conjunto de todas as palavras em A incluindo λ é frequentemente denotado por A^*. Logo, A^* é um monoide sob concatenação; ele é chamado de *monoide livre* em A.

Subsemigrupos

Seja A um subconjunto não vazio de um semigrupo S Então A é chamado de subsemigrupo de S, se A em si é um semigrupo em relação às operações em S. Uma vez que os elementos de A são também elementos de S, a Lei Associativa automaticamente é válida para os elementos de A Portanto, A é um subsemigrupo de S se, e somente se, A é fechado sob a operação em S

Exemplo B.6

(a) Considere que A e B denotam, respectivamente, o conjunto de inteiros positivos pares e ímpares. Então $(A, \times)$ e $(B, \times)$ são subsemigrupos de $(\mathbf{N}, \times)$, uma vez que A e B são fechados sob multiplicação. Por outro lado, $(A, +)$ é um subsemigrupo de $(\mathbf{N}, +)$, uma vez que A é fechado sob adição, mas $(B, +)$ não é um subsemigrupo de $(\mathbf{N}, +)$, uma vez que B não é fechado sob adição.

(b) Seja F o semigrupo livre no conjunto $A = \{a, b\}$ Considere que H consiste em todas as palavras pares, isto é, palavras com comprimento par A concatenação de duas dessas palavras também é par. Logo, H é um subsemigrupo de F

Relações de congruência e estruturas de quociente

Seja S um semigrupo, e considere que $\sim$ é uma relação de equivalência em S Lembre-se de que a relação de equivalência $\sim$ induz uma partição de S em classes de equivalência Além disso, $[a]$ denota a classe de equivalência contendo os elementos $a \in S$, e a coleção de classes de equivalência é denotada por $S/\sim$

Suponha que a relação de equivalência $\sim$ em S tem a seguinte propriedade:

Se $a \sim a'$ e $b \sim b'$, então $ab \sim a'b'$

Então $\sim$ é chamada de *relação de congruência* em S. Além disso, podemos agora definir uma operação nas classes de equivalência por meio de

$$[a] * [b] = [a * b] \quad \text{ou, simplesmente,} \quad [a]\,[b] = [ab]$$

Fora isso, essa operação em $S/\sim$ é associativa, logo, $S/\sim$ é um semigrupo. Expomos esse resultado formalmente.

Teorema B.3: Seja $\sim$ uma relação de congruência em um semigrupo S. Então $S/\sim$, as classes de equivalência sob $\sim$, formam um semigrupo sob a operação $S/\sim$.

Esse semigrupo $S/\sim$ é chamado de quociente de S por $\sim$.

Exemplo B.7

(a) Seja F o semigrupo livre em um conjunto A. Definimos $u \sim u'$ se u e u' possuírem o mesmo comprimento. Então $\sim$ é uma relação de equivalência em F. Além disso, suponha que $u \sim u'$ e $v \sim v'$, digamos,

$$l(u) = l(u') = m \quad \text{e} \quad l(v) = l(v') = n$$

Então $l(uv) = l(u'v') = m + n$ e, portanto, $uv \sim u'v'$ Logo, $\sim$ é uma relação de congruência em F.

(b) Considere os inteiros $\mathbf{Z}$ e um inteiro positivo $m > 1$ Lembre-se (Seção 11.8) de que dizemos que a é congruente a b, módulo m, escrito na forma

$$a \equiv b \pmod{m}$$

se m divide a diferença $a - b$ O Teorema 11 21 nos diz que essa relação é uma relação de equivalência em $\mathbf{Z}$. Além disso, o Teorema 11 22 nos diz que, se $a \equiv c \pmod{m}$ e $b \equiv d \pmod{m}$, então:

$$a + b \equiv c + d \pmod{m} \quad \text{e} \quad ab \equiv cd \pmod{m}$$

Em outras palavras, essa relação é de congruência em $\mathbf{Z}$.

Homomorfismo em semigrupos

Considere dois semigrupos $(S, *)$ e $(S', *')$. Uma função $f: S \to S'$ é chamada de *homomorfismo de semigrupos* ou, simplesmente, um *homomorfismo* se

$$f(a * b) = f(a) *' f(b) \quad \text{ou, simplesmente,} \quad f(ab) = f(a)f(b)$$

Suponha que f é também injetora e sobrejetora. Então f é chamado de *isomorfismo* entre S e S', e S e S' são ditos semigrupos *isomorfos*, escrito na forma $S \cong S$.

Exemplo B.8

(a) Seja M o conjunto de todas as matrizes 2×2 com entradas inteiras. O determinante de qualquer matriz $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ é denotado e definido por $\det(A) = |A| = ad - bc$. É possível provar em Álgebra Linear que o determinante é uma *função multiplicativa*, isto é, para quaisquer matrizes A e B,

$$\det(AB) = \det(A) \cdot \det(B)$$

Logo, a função determinante é um homomorfismo de semigrupos em $(M, \times)$, as matrizes sob multiplicação. Por outro lado, a função determinante não é aditiva, isto é, para algumas matrizes,

$$\det(A + B) \neq \det(A) + \det(B)$$

Logo, a função determinante não é um homomorfismo de semigrupos em $(M, +)$.

(b) A Figura B-2(a) nos dá a tabela de adição para $\mathbf{Z}_4$, os inteiros módulo 4 sob adição; e a Fig. B-2(b) nos dá a tabela de multiplicação para $S = \{1, 3, 7, 9\}$ em $\mathbf{Z}_{10}$. (Notamos que S é um sistema resíduo reduzido para os inteiros $\mathbf{Z}$ módulo 10.) Seja $f: \mathbf{Z}_4 \to S$ definido por

$$f(0) = 1, \quad f(1) = 3, \quad f(2) = 9, \quad f(3) = 7$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	
3	3	0	1	2

(a)

×	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7		9	3
9	9	7	3	1

(b)

Figura B-2

É possível mostrar que f é um homomorfismo. Uma vez que f é também injetora e sobrejetora, f é um isomorfismo. Logo, $\mathbf{Z}_4$ e S são semigrupos isomorfos.

(c) Seja $\sim$ uma relação de congruência em um semigrupo S. Seja $\phi: S \to S/\sim$ o *mapeamento natural* de S no semigrupo $S/\sim$ definido por

$$\phi(a) = [a]$$

Isto é, cada elemento a em S é associado à sua classe de equivalência $[a]$. Então, ϕ é um homomorfismo, uma vez que

$$\phi(ab) = [ab] = [a][b] = \phi(a)\phi(b)$$

Teorema fundamental de homomorfismos de semigrupos

Lembre-se de que a imagem de uma função $f: S \to S'$, escrita $f(S)$ de $\operatorname{Im} f$, consiste nas imagens dos elementos de S sob f. Logo:

$$\operatorname{Im} f = \{b \in S' \mid \text{existe } a \in S \text{ para o qual } f(a) = b\}$$

O seguinte teorema (demonstrado no Problema B.5) é fundamental à teoria de semigrupos.

Teorema B.4: Seja $f: S \to S'$ um homomorfismo de semigrupos. Seja $a \sim b$ se $f(a) = f(b)$. Então: (i) $\sim$ é uma relação de congruência em S. (ii) $S/\sim$ é isomorfo a $f(S)$.

Exemplo B.9

(a) Seja F o semigrupo livre em $A = \{a, b\}$. A função $f: F \to \mathbf{Z}$, definida por

$$f(u) = l(u)$$

é um homomorfismo. Note que $f(F) = \mathbf{N}$. Logo, $F/\sim$ é isomorfo a $\mathbf{N}$.

(b) Seja M o conjunto de matrizes 2×2 com entradas inteiras. Considere a função determinante $M \to \mathbf{Z}$. Notamos que a imagem do determinante é $\mathbf{Z}$. Segundo o Teorema B.4, $M/\sim$ é isomorfo a $\mathbf{Z}$.

Produtos de semigrupos

Sejam $(S_1, *_1)$ e $(S_2, *_2)$ semigrupos. Formamos um novo semigrupo $S = S_1 \otimes S_2$, chamado de produto direto de S_1 e S_2, como se segue.

(1) Os elementos de S vêm de $S_1 \times S_2$, isto é, são pares ordenados (a, b) onde $a \in S_1$ e $b \in S_2$.

(2) A operação $*$ em S é definida de acordo com as componentes, isto é,

$$(a, b) * (a', b') = (a *_1 a', b *_2 b') \text{ ou, simplesmente, } (a, b)(a', b') = (aa', bb')$$

É facilmente mostrado (Problema B.3) que a operação acima é associativa.

B.4 GRUPOS

Seja G um conjunto não vazio com uma operação binária (denotada por justaposição). Então G é chamado de *grupo* se os seguintes axiomas forem válidos.

[G_1] Lei Associativa: Para quaisquer a, b ou c em F, temos $(ab)c = a(bc)$.

[G_2] Elemento identidade. Existe um elemento e em G tal que $ae = ea = a$ para todo a em G.

[G_3] Inversos: Para cada a em G, existe um elemento a^{-1} em G (o inverso de a) tal que

$$aa^{-1} = a^{-1}a = e$$

Um grupo G é dito *abeliano* (ou *comutativo*) se $ab = ba$ para todo $a, b \in G$, isto é, se G satisfaz a Lei Comutativa.

Quando a operação binária é denotada por justaposição, como foi o caso acima, o grupo G é dito como sendo escrito *multiplicativamente*. Às vezes, quando G é abeliano, a operação binária é denotada por $+$ e G é dito como sendo escrito *aditivamente*. Em tal caso, o elemento identidade é denotado por 0 e é chamado de elemento *zero*; e o inverso é denotado por $-a$ e é chamado de *negativo* de a.

O número de elementos em um grupo G, denotado por $|G|$, é chamado de *ordem* de G. Em particular, G é chamado de *grupo finito* se sua ordem é finita.

Suponha que A e B são subconjuntos de um grupo G. Então escrevemos:

$$AB = \{ab \mid a \in A, b \in B\} \quad \text{ou} \quad A + B = \{a + b \mid a \in A, b \in B\}$$

Exemplo B.10

(a) Os números racionais diferentes de zero $\mathbf{Q}\backslash\{0\}$ formam um grupo abeliano sob multiplicação. O número 1 é o elemento identidade e q/p é o inverso multiplicativo do número racional p/q.

(b) Seja S o conjunto de matrizes 2×2 com entradas racionais sob operação de multiplicação de matrizes. Então S não é um grupo, uma vez que inversos nem sempre existem. Contudo, considere que G é o subconjunto de matrizes 2×2 com um determinante diferente de zero. Então G é um grupo sob multiplicação de matrizes. O elemento identidade é

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ e o inverso de } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ é } A^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix}$$

Isso é um exemplo de um grupo não abeliano, uma vez que a multiplicação de matrizes não é comutativa.

(c) Lembre-se de que $\mathbf{Z}_m$ denota o módulo de inteiros m. $\mathbf{Z}_m$ é um grupo sob adição, mas não é um grupo sob multiplicação. Contudo, considere que $\mathbf{U}_m$ denota um sistema de resíduo reduzido módulo m que consiste nesses inteiros relativamente primos de m. Então $\mathbf{U}_m$ é um grupo sob multiplicação (módulo m). A Figura B-3 nos dá a tabela de multiplicação para $\mathbf{U}_{12} = \{1, 5, 7, 11\}$.

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Figura B-3

	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
ε	ε	ϕ	σ_2	σ_3	ϕ_1	ϕ_2
σ_1	σ_1	ε	ϕ_1	ϕ_2	σ_2	σ_3
σ_2	σ_2	ϕ_2	ε	ϕ_1	σ_3	σ_1
σ_3	σ_3	ϕ_1	ϕ_2	ε	σ_1	σ_2
ϕ_1	ϕ_1	σ_3	σ_1	σ_2	ϕ_2	ε
ϕ_2	ϕ_2	σ_2	σ_3	σ_1	ε	ϕ_1

Figura B-4

Grupo simétrico S_n

Um mapeamento um para um σ do conjunto $\{1, 2, \ldots, n\}$ em si é chamado de *permutação*. Tal permutação pode ser denotada, como se segue, onde $j_i = \sigma(i)$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

O conjunto de todas as permutações nesse estilo é denotado por S_n e existem $n! = n(n-1) \cdot \ldots \cdot 2 \cdot 1$ delas. A composição e inversos de permutações em S_n pertencem a S_n, a função identidade ε pertence a S_n. Logo, S_n forma um grupo sob composição de funções chamado de *grupo simétrico de grau n*.

O grupo simétrico S_3 possui $3! = 6$ elementos, como se segue:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

A tabela de multiplicação de S_3 aparece na Fig. B-4.

MAP(A), PERM(A) e AUT(A)

Seja A um conjunto não vazio. A coleção MAP(A) de todas as funções (mapeamentos) $f: A \to A$ é um semigrupo sob composição de funções, não é um grupo, uma vez que algumas funções podem não ter inversos. Contudo, o semigrupo PERM(A) de todas as correspondências um para um de A com ele próprio (chamado de *permutações* de A) é um grupo sob composição de funções.

Além disso, suponha que A contém algum tipo de estrutura geométrica ou algébrica, por exemplo, A pode ser o conjunto de vértices de um gráfico ou A pode ser um conjunto ordenado, ou um semigrupo. Então, o conjunto AUT(A) de todos os isomorfismos de A com ele mesmo (chamado de *automorfismos* de A) é também um grupo sob composição de funções.

B.5 SEMIGRUPOS, SUBGRUPOS NORMAIS E HOMOMORFISMOS

Seja H um subconjunto de um grupo G. Então H é chamado de *subgrupo* de G, se H é um grupo sob operação de G. Existem critérios simples para determinar subgrupos.

Proposição B.5: Um subconjunto H de um grupo G é um subgrupo de G se:

(i) O elemento identidade $e \in H$.
(ii) H é fechado sob a operação de G, isto é, se $a, b \in H$, então $ab \in H$.
(iii) H é fechado por inversos, isto é, se $a \in H$, então $a^{-1} \in H$.

Todo grupo G possui os subgrupos $\{e\}$ e o próprio G. Qualquer outro subgrupo de G é chamado de *subgrupo não trivial*.

Co-conjuntos

Suponha que H é um subconjunto de G e que $a \in G$. Então, o conjunto

$$Ha = \{ha \mid h \in H\}$$

é chamado de *co-conjunto à direita* de H. (Analogamente, aH é chamado de *co-conjunto à esquerda* de H.) Temos os resultados importantes a seguir (provados nos Problemas B.13 e B.15).

Teorema B.6: Seja H um subgrupo de um grupo G. Então os co-conjuntos à direita Ha formam uma partição de G.

Teorema B.7 (Lagrange): Seja H um subgrupo de um grupo finito G. Então a ordem de H divide a ordem de G.

O número de co-conjuntos à direita de H em G, chamado de índice de H em G, é igual ao número de co-conjuntos à esquerda de H em G, e ambos os números são iguais a $|G|$ divididos por $|H|$.

Subgrupos normais

A definição a seguir se aplica.

Definição B.2: Um subgrupo H de G é um subgrupo *normal* se $a^{-1}Ha \subseteq H$, para todo $a \in G$ ou, de forma equivalente, se $aH = Ha$, ou seja, se os co-conjuntos à esquerda e à direita coincidirem.

Note que todo subgrupo de um grupo abeliano é normal.

A importância dos subgrupos normais vem do seguinte resultado (provado no Problema B.17).

Teorema B.8: Seja H um subgrupo normal de um grupo G. Então os co-conjuntos de H formam um grupo sobre multiplicação de co-conjuntos:

$$(aH)(bH) = abH$$

Esse grupo é chamado de *grupo quociente* e é denotado por G/H.

Suponha que a operação em G é adição ou, em outras palavras, G é escrito de forma aditiva. Então, os co-conjuntos de um subgrupo H de G são da forma $a + H$. Além disso, se H é um subgrupo normal de G, então os co-conjuntos formam um grupo sob adição de co-conjuntos, isto é,

$$(a + H) + (b + H) = (a + b) + H$$

Exemplo B.11

(a) Considere o grupo de permutação S_3 de grau 3 recém-investigado. O conjunto $H = \{\varepsilon, \sigma_1\}$ é um subgrupo de S_3. Seus co-conjuntos à esquerda e à direita estão listados a seguir:

Co-conjuntos à Direita	**Co-conjuntos à Esquerda**
$H = \{\varepsilon, \sigma_1\}$	$H = \{\varepsilon, \sigma_1\}$
$H\phi_1 = \{\phi_1, \sigma_2\}$	$\phi_1 H = \{\phi_1, \sigma_3\}$
$H\phi_2 = \{\phi_2, \sigma_3\}$	$\phi_2 H = \{\phi_2, \sigma_2\}$

Observe que os co-conjuntos à direita e à esquerda são distintos, logo, H não é um subgrupo normal de S_3.

(b) Considere o grupo G de matrizes 2×2 com entradas racionais e determinantes diferentes de zero. (Veja o exemplo A.10.) Seja H o subconjunto de G, consistindo em matrizes cuja entrada superior direita é zero; isto é, matrizes da forma

$$\begin{bmatrix} a & 0 \\ c & d \end{bmatrix}$$

Então H é um subgrupo de G, uma vez que H está fechado sob multiplicação e inversos, e $I \in H$. Contudo, H não é um subgrupo normal, uma vez que, por exemplo, o produto a seguir não pertence a H:

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} -1 & -4 \\ 1 & 3 \end{bmatrix}$$

Por outro lado, seja K um subconjunto de G que consiste em matrizes com determinante igual a 1. É possível mostrar que K é também um subgrupo de G. Além disso, para qualquer matriz X em G e qualquer matriz A em K, temos

$$\det(X^{-1}AX) = 1$$

Logo, $X^{-1}AX$ pertence a K, então, K é um subgrupo normal de G.

Inteiros módulo *m*

Considere o grupo $\mathbf{Z}$ de inteiros sob adição. Seja H a notação para os múltiplos de 5, isto é,

$$H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

Então H é um subgrupo (obrigatoriamente normal) de $\mathbf{Z}$. Os co-conjuntos de H em $\mathbf{Z}$ aparecem na Fig. B-5(a). Segundo o Teorema B-8, $\mathbf{Z}/H = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ é um grupo sob adição de co-conjuntos, sua tabela de adição aparece na Fig. B-5(b).

Esse grupo de quocientes $\mathbf{Z}/H$ é referido como os inteiros módulo 5 e é frequentemente denotado por $\mathbf{Z}_5$. Analogamente, para qualquer n inteiro positivo, existe um grupo quociente $\mathbf{Z}_n$ chamado de *inteiros módulo n*.

$\bar{0} = 0 + H = H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$
$\bar{1} = 1 + H = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$
$\bar{2} = 2 + H = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$
$\bar{3} = 3 + H = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$
$\bar{4} = 4 + H = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$

(a)

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

(b)

Figura B-5

Subgrupos cíclicos

Seja G um grupo qualquer e a um elemento qualquer de G. Como é usual, definimos $a^0 = e$ e $a^{n+1} = a^n \cdot a$. Claramente, $a^m a^n = a^{m+n}$ e $(a^m)^n = a^{mn}$, para quaisquer inteiros m e n. Seja S a notação para o conjunto de todas as potências de a, isto é

$$S = \{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots\}$$

Então S é um subgrupo de G, chamado de grupo cíclico gerado por a. Denotamos esse grupo na forma $gp(a)$.

Além disso, suponha que as potências de a não são distintas, digamos $a^r = a^s$ com, por exemplo, $r > s$. Então, $a^{r-s} = e$ onde $r, s > 0$. O menor m inteiro positivo tal que $a^m = e$ é chamado de *ordem* de a e será denotado por $|a|$. Se $|a| = m$, então o subgrupo cíclico $gp(a)$ possui m elementos, como se segue:

$$gp(a) = \{e, a, a^2, a^3, \ldots, a^{m-1}\}$$

Considere, por exemplo, o elemento ϕ_1 no grupo simétrico S_3 discutido anteriormente. Então:

$$\phi_1{}^1 = \phi_1, \quad \phi_1{}^2 = \phi_2, \quad \phi_1{}^3 = \phi_2 \cdot \phi_1 = e$$

Logo, $|\phi_1| = 3$ e $gp(\phi_1) = \{e, \phi_1, \phi_2\}$. Observe que $|\phi_1|$ divide a ordem de S_3. Isso é usualmente verdade, isto é, para qualquer elemento a em um grupo G, $|a|$ é igual à ordem de $gp(a)$ e, portanto, $|a|$ divide $|G|$ segundo o Teorema B.7 de Lagrange. Observamos também que um grupo G é considerado *cíclico* se ele possui um elemento a tal que $G = gp(a)$.

Conjuntos geradores, geradores

Considere qualquer subconjunto A de um grupo G. Seja $gp(A)$ a notação do conjunto de todos os elementos x em G, tal que x é igual a um produto de elementos, onde cada elemento é oriundo do conjunto $A \cup A^{-1}$ (onde A^{-1} denota o conjunto de inversos de elementos de A). Isto é,

$$gp(A) = \{x \in G \mid x = b_1 b_2 \ldots b_m \text{ onde cada } b_i \in A \cup A^{-1}\}$$

Então $gp(A)$ é um subgrupo de G com um *conjunto gerador* A. Em particular, A é dito gerador do grupo G se $G = gp(A)$, isto é, se todo g em G é um produto de elementos de $A \cup A^{-1}$. Dizemos que A é um *conjunto mínimo de geradores* de G, se A gera G, e se nenhum conjunto com menos elementos de A fizer o mesmo. Por exemplo, as permutações $a = \sigma_1$ e $b = \phi_1$ formam um conjunto mínimo de geradores do grupo simétrico S_3 (Fig. B-4). Especificamente,

$$e = a^2, \quad \sigma_1 = a, \quad \sigma_2 = ab, \quad \sigma_3 = ab^2, \quad \phi_1 = b, \quad \phi_2 = b^2$$

e S_3 não é cíclico, então ele não pode ser gerado por um único elemento.

Homomorfismos

Um mapeamento f de um grupo G em um grupo G' é chamado de homomorfismo se, para todo $a, b \in G$,

$$f(ab) = f(a)f(b)$$

Além disso, se f é injetora e sobrejetora, então f é chamado de *isomorfismo*; e G e G' são ditos *isomorfos*, o que é escrito na forma $G \simeq G'$.

Se $f: G \to G'$ é um isomorfismo, então o núcleo de f, escrito na forma $\operatorname{Ker} f$, é o conjunto de elementos cuja imagem é o elemento identidade e' de G'; isto é,

$$\operatorname{Ker} f = \{a \in G \mid f(a) = e'\}$$

Lembre-se de que a imagem de f, escrita na forma $f(G)$ ou $\operatorname{Im} f$, consiste nas imagens dos elementos sob f, isto é,

$$\operatorname{Im} f = \{b \in G' \mid \text{ existe um } a \in G \text{ para o qual } f(a) = b\}.$$

O teorema a seguir (demonstrado no Problema B.19) é fundamental à teoria de grupos.

Teorema B.9: Suponha que $f: G \to G'$ é um homomorfismo com núcleo K. Então K é um subgrupo normal de G, e o grupo quociente G/K é isomorfo a $f(G)$.

Exemplo B.12

(a) Seja G o grupo de números reais sob adição, e seja G' o grupo de números positivos reais sob multiplicação. O mapeamento $f: G \to G'$, definido por $f(a) = 2^a$ é um homomorfismo, pois

$$f(a+b) = 2^{a+b} = 2^a 2^b = f(a)f(b)$$

Na verdade, f também é injetora e sobrejetora, logo, G e G' são isomorfos.

(b) Seja a qualquer elemento em um grupo G. A função $f: \mathbf{Z} \to G$, definida por $f(n) = a^n$ é um homomorfismo, uma vez que

$$f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$$

A imagem de f é $gp(a)$, o subgrupo cíclico gerado por a. Segundo o Teorema B.9,

$$gp(a) \cong \mathbf{Z}/\mathbf{K}$$

onde K é o núcleo de f. Se $K = \{0\}$, então $gp(a) \cong \mathbf{Z}$. Por outro lado, se m é a ordem de a, então $K = \{$múltiplos de $m\}$ e, portanto, $gp(a) \cong \mathbf{Z}_m$. Em outras palavras, qualquer grupo cíclico é isomorfo aos inteiros $\mathbf{Z}$ sob adição, ou a $\mathbf{Z}_m$, os inteiros sob adição módulo m.

B.6 ANÉIS, DOMÍNIOS DE INTEGRIDADE E CORPOS

Seja R um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por justaposição). Então, R é chamado de *anel* se os axiomas a seguir forem satisfeitos:

[$\mathbf{R}_1$] Para qualquer a, b e $c \in R$, temos $(a+b)+c = a+(b+c)$.

[$\mathbf{R}_2$] Existe um elemento $0 \in R$, chamado de elemento *zero*, tal que, para todo $a \in R$,

$$a + 0 = 0 + a = a.$$

[$\mathbf{R}_3$] Para cada $a \in R$, existe um elemento $-a \in R$, chamado de *negativo* de a, tal que

$$a + (-a) = (-a) + a = 0$$

[$\mathbf{R}_4$] Para qualquer $a, b \in R$, temos $a + b = b + a$.

[$\mathbf{R}_5$] Para qualquer a, b e $c \in R$, temos $(ab)c = a(bc)$.

[$\mathbf{R}_6$] Para qualquer a, b e $c \in R$, temos: (i) $a(b+c) = ab + ac$ e (ii) $(b+c)a = ba + ca$.

Observe que os axiomas [$\mathbf{R}_1$] até o [$\mathbf{R}_4$] podem ser resumidos se dissermos que R é um grupo abeliano sob adição.

Subtração é definida em R por $a - b = a + (-b)$.

É possível provar que $a \cdot 0 = 0 \cdot a = 0$ para todo $a \in R$ (Problema B.21).

Um subconjunto S de R é um *subanel* de R, se S em si for também um anel sob as operações em R. Notamos que S é um subanel de R se: (i) $0 \in S$ e (ii) para quaisquer $a, b \in S$, temos $a - b \in S$ e $ab \in S$.

Tipos especiais de anéis

Esta subseção define vários tipos diferentes de anéis, incluindo domínios de integridade e corpos.

R é chamado de *anel comutativo* se $ab = ba$ para todo $a, b \in R$.

R é chamado de *anel com um elemento identidade 1* se o elemento 1 possui a propriedade que $a \cdot 1 = 1 \cdot a = a$ para todo elemento $a \in R$. Em tal caso, um elemento $a \in R$ é chamado de *unidade* se a possuir um inverso multiplicativo, isto é, um elemento a^{-1} em R tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

R é chamado de um *anel com divisores zero* se existirem elementos a e $b \in R$ diferentes de zero de tal forma que $ab = 0$. Neste caso, a e b são chamados de *divisores zero*.

Definição B.3: Um anel comutativo R é um *domínio de integridade* se R não possui divisores zero, isto é, se $ab = 0$ implica $a = 0$ ou $b = 0$.

Definição B.4: Um anel comutativo R com um elemento identidade 1 (não igual a 0) é um corpo se todo $a \in R$ diferente de zero for uma unidade, isto é, possui um inverso multiplicativo.

Um corpo é, necessariamente, um domínio de integridade; pois, se $ab = 0$ e $a \neq 0$, então

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0$$

Observamos que um corpo pode também ser visto como um anel comutativo no qual os elementos diferentes de zero formam um grupo sob multiplicação.

Exemplo B.13

(a) O conjunto $\mathbf{Z}$ de inteiros com as operações usuais de adição e multiplicação é o exemplo clássico de um domínio de integridade (com um elemento identidade). As unidades em $\mathbf{Z}$ são apenas 1 e −1, isto é, nenhum outro elemento em $\mathbf{Z}$ possui um inverso multiplicativo.

(b) O conjunto $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$ sob a operação de adição e multiplicação módulo m é um anel, ele é chamado de *anel de inteiros módulo m*. Se m é um primo, então $\mathbf{Z}_m$ é um corpo. Por outro lado, se m não é primo, então $\mathbf{Z}_m$ não possui divisores zero. Por exemplo, no anel $\mathbf{Z}_6$,

$$2 \cdot 3 = 0, \quad \text{mas} \quad 2 \not\equiv 0 \pmod 6 \quad \text{e} \quad 3 \not\equiv 0 \pmod 6$$

(c) Os números racionais $\mathbf{Q}$ e reais $\mathbf{R}$ formam, cada um, um corpo em relação às operações usuais de adição e multiplicação.

(d) Seja M a notação de um conjunto com matrizes 2×2 com entradas inteiras ou reais. Então, M é um anel não comutativo com divisores zero sob as operações de multiplicação e adição de matrizes. M possui um elemento identidade, que é a matriz identidade.

(e) Seja R qualquer anel. Então o conjunto $R[x]$ de todos os polinômios sobre R é um anel em relação às operações usuais de adição e multiplicação de polinômios. Além disso, se R é um domínio de integridade, então $R[x]$ também o é.

Ideais

Um subconjunto J de um anel R é um *ideal* em R se as três propriedades a seguir forem válidas.

(i) $0 \in J$.
(ii) Para quaisquer a e $b \in J$, temos $a - b \in J$.
(iii) Para qualquer $r \in R$ e $a \in J$, temos ra e $ar \in J$.

Note primeiro que J é um subanel de R. Além disso, J é um subgrupo (necessariamente normal) do grupo aditivo de R. Logo, podemos formar a seguinte coleção de co-conjuntos, que formam uma partição de R:

$$\{a + J \mid a \in R\}$$

A importância de ideais provém do seguinte teorema que é análogo ao Teorema B.7 para subgrupos normais.

Teorema B.10: Seja J um ideal em um anel R. Então os co-conjuntos $\{a + J \mid a \in R\}$ formam um anel sob as operações de co-conjuntos.

$$(a + J) + (b + J) = a + b + J \quad \text{e} \quad (a + J)(b + J) = ab + J$$

Esse anel é denotado por R/J e é chamado de *anel quociente*.

Agora, seja R um anel comutativo com um elemento identidade 1. Para qualquer $a \in R$, o seguinte conjunto é um ideal.

$$(a) = \{ra \mid r \in R\} = aR$$

É chamado de *ideal principal gerado* por a. Se todo ideal em R é um ideal principal, então R é chamado de *anel ideal principal*. Em particular, se R é também um domínio integral, então ele é chamado de *domínio ideal principal* (DIP).

Exemplo B.14

(a) Considere o anel $\mathbf{Z}$ de inteiros. Então, todo ideal J em $\mathbf{Z}$ é um ideal principal, isto é, $J = (m) = m\mathbf{Z}$, para algum inteiro m. Logo, $\mathbf{Z}$ é um domínio ideal principal (DIP). O anel quociente $\mathbf{Z_m} = \mathbf{Z}/(m)$ é simplesmente o anel de inteiros módulo m. Apesar de $\mathbf{Z}$ ser um domínio de integridade (não há divisores zero), o anel quociente $\mathbf{Z_m}$ pode possuir divisores zero, por exemplo, 2 e 3 são divisores zero em $\mathbf{Z_6}$.

(b) Seja R qualquer anel. Então $\{0\}$ e R são ideais. Em particular, se R é um corpo, então $\{0\}$ e R são os únicos ideais.

(c) Seja K um corpo. Então o anel $K[x]$ de polinômios sobre K é um domínio ideal principal (DIP). Por outro lado, o anel $K[x, y]$ de polinômios com duas variáveis não é um domínio ideal principal (DIP).

Homomorfismos de anéis

Um mapeamento f de um anel R em um anel R' é chamado de *homomorfismo de anéis* ou, simplesmente, de *homomorfismo* se, para todo a e $b \in R$,

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b)$$

Além disso, se f é injetora e sobrejetora, então f é chamada de *isomorfismo*, e R e R' são ditos *isomorfos*, escrito na forma $R \cong R'$.

Suponha que $f: R \to R'$ é um isomorfismo. Então o núcleo de f, escrito como Ker f, é o conjunto de elementos cujas imagens são o elemento zero 0 de R', isto é,

$$\text{Ker}\, f = \{r \in R \mid f(r) = 0\}$$

O teorema a seguir (análogo ao Teorema B.9 para grupos) é fundamental à teoria de anéis.

Teorema B.11: Seja $f: R \to R'$ um homomorfismo de anéis com núcleo K. Então K é um ideal em R, e o anel quociente R/K é isomorfo a $f(R)$.

Divisibilidade em domínios de integridade

Agora considere que D é um domínio de integridade. Dizemos que B divide A em D se $a = bc$ para algum $c \in D$. Um elemento $u \in D$ é chamado de *unidade* se u dividir 1, ou seja, se u possui um inverso multiplicativo. Um elemento $b \in D$ é chamado de *associativo* de $a \in D$ se $b = ua$ para alguma unidade $u \in D$. Uma não unidade $p \in D$ é dita *irredutível* se $p = ab$ implica a ou b como sendo uma unidade.

Um domínio de integridade D é chamado de *domínio de fatorização única* (DFU), se toda não unidade $a \in D$ puder ser escrita de forma única (a menos de associados e ordem) como um produto de elementos irredutíveis.

Exemplo B.15

(a) O anel $\mathbf{Z}$ de inteiros é o clássico exemplo de um domínio de fatoração única. As unidades de $\mathbf{Z}$ são 1 e -1. Os únicos associados de $n \in \mathbf{Z}$ são n e $-n$. Os elementos irredutíveis de $\mathbf{Z}$ são os números primos.

(b) O conjunto $D = \{a + b\sqrt{13} \mid a, b, \text{ inteiros}\}$ é um domínio de integridade. As unidades de D, a seguir:

$$\pm 1, \quad 18 \pm 5\sqrt{13}, \quad -18 \pm 5\sqrt{13}$$

Os elementos 2, $3 - \sqrt{13}$ e $-3 - \sqrt{13}$ são irredutíveis em D. Observe que

$$4 = 2 \cdot 2 = (3 - \sqrt{13})(-3 - \sqrt{13})$$

Logo, D não é um domínio de fatoração única. (Ver o Problema B.97.)

B.7 POLINÔMIOS SOBRE UM CORPO

Esta seção investiga polinômios cujos coeficientes se originam a partir de algum domínio de integridade ou corpo K. Em particular, mostramos que polinômios sobre um corpo K possuem várias das mesmas propriedades dos inteiros.

Definições básicas

Seja K um domínio de integridade ou um corpo. Formalmente, um polinômio f sobre K é uma sequência infinita de elementos de K, na qual todos, com exceção de um número finito dela, é 0; isto é,

$$f = (\ldots, 0, a_n, \ldots, a_1, a_0) \quad \text{ou, de forma equivalente,} \quad f(t) = a_n t^n + \cdots + a_1 t + a_0$$

onde o símbolo t é usado como uma indeterminada. A entrada a_k é chamada de k-ésimo coeficiente de f. Se n é o maior inteiro para o qual $a \neq 0$, então dizemos que o grau de f é n, escrito na forma $\deg(f) = n$. Também chamamos a_n de coeficiente principal de f. Se $a_n = 1$, chamamos f de um polinômio *mônico*. Por outro lado, se todo coeficiente de f é 0, então f é chamado de polinômio *zero*, escrito na forma $f = 0$. O grau do polinômio zero não é definido.

Seja $K[t]$ uma coleção de todos os polinômios $f(t)$ sobre K. Considere os polinômios

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad \text{e} \quad g(t) = b_m t^m + \cdots + b_1 t + b_0$$

Então a soma $f + g$ é o polinômio obtido pela soma dos coeficientes correspondentes, isto é, se $m \leq n$, então

$$f(t) + g(t) = a_n t^n + \cdots + (a_m + b_m) t^m + \cdots + (a_1 + b_1) t + (a_0 + b_0)$$

Além disso, o produto de f e g é o polinômio

$$f(t) g(t) = (a_n b_m) t^{n+m} + \cdots + (a_1 b_0 + a_0 b_1) t + (a_0 b_0)$$

Isto é,

$$f(t) g(t) = c_{n+m} t^{n+m} + \cdots + c_1 t + c_0 \quad \text{onde} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i} = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$$

O conjunto K de escalares é visto como um subconjunto de $K[t]$. Especificamente, identificamos o escalar $a_0 \in K$ com o polinômio

$$f(t) = a_0 \quad \text{ou} \quad a_0 = (\cdots, 0, 0, a_0)$$

Então os operadores de adição e multiplicação escalar são preservados por essa identificação. Logo, o mapeamento $\psi: K \to K[t]$, definido por $\psi(a_0) = a_0$, é um isomorfismo que engloba K em $K[t]$.

Teorema B.12: Seja K um domínio de integridade. Então $K[t]$, sob as operações de adição e multiplicação de polinômios, é um anel comutativo com um elemento identidade 1.

O resultado simples a seguir possui consequências importantes.

Lema B.13: Suponha que f e g são polinômios sobre um domínio integral K. Então

$$\deg(fg) = \deg(f) + \deg(g).$$

A prova é resultado direto da definição do produto de polinômios. Ou seja, suponha que

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad \text{e} \quad g(t) = b_m t^m + \cdots + b_1 t + b_0$$

onde $a_n \neq 0$ e $b_n \neq 0$. Logo, $\deg(f) = n$ e $\deg(g) = m$. Então

$$f(t) g(t) = a_n b_m t^{n+m} + \text{termos de grau inferior}$$

Além disso, uma vez que K é um domínio de integridade com nenhum divisor zero, $a_n b_m \neq 0$. Logo,

$$\deg(fg) = m + n = \deg(f) + \deg(g)$$

e o lema é provado.

A proposição a seguir lista várias propriedades de nossos polinômios. (Lembre-se de que um polinômio g é dito *divisor* de um polinômio f se existir um polinômio h tal que $f(t) = g(t)h(t)$.)

Proposição B.14: Seja K um domínio de integridade, e considere que f e g são polinômios sobre K.

(i) $K[t]$ é um domínio de integridade.
(ii) As unidades de $K[t]$ são unidades em K.
(iii) Se g divide f, então $\deg(g) \leq \deg(f)$ ou $f \equiv 0$.
(iv) Se g divide f e f divide g, então $f(t) = kg(t)$ onde k é uma unidade em K
(v) Se d e d' são polinômios mônicos, tal que d divide d' e d' divide d, então $d = d'$.

Algoritmos euclidianos, raízes de polinômios

Esta subseção discute as raízes de um polinômio $f(t)$, onde assumimos agora que os coeficientes de $f(t)$ provêm de um corpo K. Lembre-se de que um escalar $a \in K$ é uma *raiz* de um polinômio $f(t)$ se $f(a) = 0$. Começamos, em primeiro lugar, com um importante teorema que é muito similar ao teorema correspondente para os inteiros $\mathbf{Z}$.

Teorema B.15 (Algoritmo de divisão euclidiana): Sejam $f(t)$ e $g(t)$ polinômios sobre um corpo K com $g(t) \neq 0$. Então existem polinômios $q(t)$ e $r(t)$ tais que

$$f(t) = q(t)g(t) + r(t)$$

onde nem $r(t) \equiv 0$, tampouco $\deg(r) < \deg(g)$.

O teorema acima (demonstrado no Problema B.30) formaliza o processo conhecido como "divisão longa". O polinômio $q(t)$ é chamado de *quociente* e o polinômio $r(t)$ é chamado de *resto* quando $f(t)$ é divido por $g(t)$.

Corolário B.16 (Teorema do resto): Suponha que $f(t)$ é dividido por $g(t) = t - a$. Então $f(a)$ é o resto.

A demonstração é resultado direto do Algoritmo euclidiano. Isto é, dividindo $f(t)$ por $t - a$, temos

$$f(t) = q(t)(t - a) + r(t)$$

onde $\deg(r) < \deg(t - a) = 1$. Logo, $r(t) = r$ é um escalar. Substituindo $t = a$ na equação por $f(t)$, implica

$$f(a) = q(a)(a - a) + r = q(t) \cdot 0 + r = r$$

Logo, $f(a)$ é o resto, como dito.

O Corolário B.16 também nos diz que $f(a) = 0$ se, e somente se, o resto $r = r(t) \equiv 0$. Consequentemente.

Corolário B.17 (Teorema de fatoração): O escalar $a \in K$ é uma raiz de $f(t)$ se, e somente se, $t - a$ é um fator de $f(t)$.

O próximo teorema (demonstrado no Problema B.31) nos diz o número de possíveis raízes de um polinômio.

Teorema B.18: Suponha que $f(t)$ é um polinômio sobre um corpo K e $\deg(f) = n$. Então $f(t)$ possui, no máximo, n raízes.

O teorema a seguir (demonstrado no Problema B.32) é a principal ferramenta para encontrar raízes racionais de um polinômio com coeficientes inteiros.

Teorema B.19: Suponha que o número racional p/q (reduzido a seus menores termos) é uma raiz do polinômio

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

onde todos os coeficientes $a_n, \ldots, a_1, a_0$ são inteiros. Então p divide o termo constante a_0 e q divide o coeficiente principal a_n. Em particular, se $c = p/q$ é um inteiro, então c divide o termo constante a_0.

Exemplo B.16

(a) Suponha que $f(t) = t^3 + t^2 - 8t + 4$. Assumindo que $f(t)$ possui uma raiz racional, encontre todas as raízes de $f(t)$.

Uma vez que o coeficiente principal é 1, as raízes racionais de $f(t)$ devem ser inteiros que estão entre ± 1, ± 2, ± 4. Note que $f(1) \neq 0$ e $f(-1) \neq 0$. Por meio de divisão sintética ou dividindo por $t - 2$, temos

$$\begin{array}{r|rrrrrrr} 2 & 1 & + & 1 & - & 8 & + & 4 \\ & & & 2 & + & 6 & - & 4 \\ \hline & 1 & + & 3 & - & 2 & + & 0 \end{array}$$

Portanto, $t = 2$ é uma raiz e $f(t) = (t - 2)(t^2 + 3t - 2)$. Usando a fórmula quadrática para $t^2 + 3t - 2 = 0$, obtemos as três raízes a seguir de $f(t)$:

$$t = 2, \quad t = (-3 + \sqrt{17})/2, \quad t = (-3 - \sqrt{17})/2$$

(b) Suponha que $h(t) = t^4 - 2t^3 + 11t - 10$. Encontre todas as raízes reais de $h(t)$, assumindo que existam duas raízes inteiras.

As raízes inteiras devem estar entre ± 1, ± 2, ± 5, ± 10. Por meio de divisão sintética (ou dividindo por $t - 1$ e, em seguida, por $t + 2$), temos

$$\begin{array}{r|rrrrrrrrr} 1 & 1 & - & 2 & + & 0 & + & 11 & - & 10 \\ & & & 1 & - & 1 & - & 1 & + & 10 \\ \hline -2 & 1 & - & 1 & - & 1 & + & 10 & + & 0 \\ & & - & 2 & + & 6 & - & 10 & & \\ \hline & 1 & - & 3 & + & 5 & + & 0 & & \end{array}$$

Logo, $t = 1$ e $t = -2$ são raízes e $h(t) = (t - 1)(t + 2)(t^2 - 3t + 5)$. A fórmula quadrática com $t^2 - 3t + 5$ nos diz que não existem outras raízes reais. Isto é, $t = 1$ e $t = -2$ são as únicas raízes reais de $h(t)$.

$K[t]$ como um domínio ideal principal e domínio de fatoração única

Os teoremas a seguir (demonstrados nos problemas B.33 e B.34) se aplicam.

Teorema B.20: O anel $K[t]$ de polinômios sobre um corpo K é um domínio ideal principal (DIP). Isto é, se J é um ideal em $K[t]$, então existe um único polinômio mônico d que gera J, isto é, todo polinômio f em J é um múltiplo de d.

Teorema B.21: Sejam f e g polinômios em $K[t]$, ambos não são zero. Então existe um único polinômio mônico d tal que:

(i) d divide tanto f quanto g. (ii) Se d' divide f e g, então d' divide d.

O polinômio d no Teorema B.21 é chamado de *máximo divisor comum* de f e g, escrito na forma $d = mdc(f, g)$. Se $d = 1$, então f e g são ditos *relativamente primos*.

Corolário B.22: Seja d o máximo divisor comum de f e g. Então existem polinômios m e n tal que $d = mf + ng$. Em particular, se f e g são relativamente primos, então existem polinômios m e n tal que $mf + ng = 1$.

Um polinômio $p \in K[t]$ é dito *irredutível* se p não é um escalar e se $p = fg$ implica f ou g como escalar. Em outras palavras, p é irredutível se seus únicos divisores são associados (múltiplos escalares). O lema a seguir (provado no Problema B.36) se aplica.

Lema B.23: Suponha que $p \in K[t]$ é irredutível. Se p divide o produto fg dos polinômios f e g em $K[t]$, então p divide f ou p divide g. De forma mais geral, se p divide o produto $f_1 f_2 \ldots f_n$ de n polinômios, então p divide um deles.

O próximo teorema (demonstrado no Problema B.37) declara que os polinômios sobre um corpo formam um *domínio de fatoração única* (DFU).

Teorema B.24 (Teorema de fatoração única). Seja f um polinômio não nulo em $K[t]$. Então f pode ser escrito unicamente (exceto quanto à ordem) como um produto

$$f = kp_1p_2 \dots p_n$$

onde $k \in K$ e os p's são polinômios mônicos irredutíveis em $K[t]$.

Teorema Fundamental da Álgebra

A demonstração do teorema a seguir está além do objetivo deste texto.

Teorema Fundamental da Álgebra: Qualquer polinômio diferente de zero $f(t)$ sobre o corpo complexo **C** possui uma raiz em **C**. Logo, $f(t)$ pode ser escrito unicamente (exceto quanto à ordem) como um produto

$$f(t) = k(t - r_1)(t - r_2) \cdots (t - r_n)$$

onde o k e o r_i são números complexos e $\deg(f) = n$.

O teorema acima é certamente inválido para o corpo dos reais **R**. Por exemplo, $f(t) = t^2 + 1$ é um polinômio sobre R, mas $f(t)$ não possui raiz real.

O teorema a seguir (demonstrado no Problema B.38) se aplica.

Teorema B.25: Suponha que $f(t)$ é um polinômio sobre o corpo **R**, e suponha que o número complexo $z = a + bi$, $b \neq 0$, é uma raiz de $f(t)$. Então o conjugado complexo $\bar{z} = a - bi$ é também uma raiz de $f(t)$. Logo, a seguir, está um fator de $f(t)$:

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

O teorema a seguir é resultado direto do Teorema B.25 e do Teorema Fundamental da Álgebra.

Teorema B.26: Seja $f(t)$ um polinômio diferente de zero sobre o corpo dos reais **R**. Então, $f(t)$ pode ser escrito unicamente (exceto quanto à ordem) como um produto

$$f(t) = kp_1(t)p_2(t) \cdots p_n(t)$$

onde o $k \in \mathbf{R}$ e o $p_i(t)$ são polinômios mônicos reais de grau 1 ou 2.

Exemplo B.17 Seja $f(t) = t^4 - 3t^3 + 6t^2 + 25t - 39$. Encontre todas as raízes de $f(t)$, considerando que $t = 2 + 3i$ é uma raiz.

Uma vez que $2 + 3i$ não é uma raiz, e $c(t) = t^2 - 4t + 13$ é um fator de $f(t)$. Dividindo $f(t)$ por $c(t)$, temos

$$f(t) = (t^2 - 4t + 13)(t^2 + t - 3)$$

A fórmula quadrática com $t^2 + t - 3$ nos dá as outras raízes de $f(t)$. Isto é, as quatro raízes de $f(t)$ são as que seguem.

$$t = 2 + 3i, \quad t = 2 - 3i, \quad t = (-1 + \sqrt{13})/2, \quad t = (-1 - \sqrt{13})/2$$

Problemas Resolvidos

Operações e semigrupos

B.1 Considere o conjunto **Q** de número racionais, e considere que $*$ é a operação em **Q** definida por

$$a * b = a + b - ab$$

(*a*) Encontre: (i) $3 * 4$, (ii) $2 * (-5)$; (iii) $7 * (1/2)$.

(*b*) (**Q**, $*$) é um semigrupo? Ele é comutativo?

(c) Encontre o elemento identidade para $*$.

(d) Algum dos elementos em **Q** possui um inverso? Qual?

(a) (i) $3 * 4 = 3 + 4 - 3(4) = 3 + 4 - 12 = -5$

(ii) $2 * (-5) = 2 + (-5) + 2(-5) = 2 - 5 + 10 = 7$

(iii) $7 * (1/2) = 7 + (1/2) - 7(1/2) = 4$

(b) Temos:

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc = a + b + c - ab - ac - bc + abc \\ a * (b * c) &= a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc\end{aligned}$$

Logo, $*$ é associativa e $(\mathbf{Q}, *)$ é um semigrupo. Além disso,

$$a * b = a + b - ab = b + a - ba = b * a$$

Então, $(\mathbf{Q}, *)$ é um semigrupo comutativo.

(c) Um elemento e é um elemento identidade se $a * e = a$ para todo $a \in \mathbf{Q}$. Calcule como se segue:

$$a * e = a, \quad a + e - ae = a, \quad e - ea = 0, \quad e(1 - a) = 0, \quad e = 0$$

Logo, 0 é o elemento identidade.

(d) Para a possuir um inverso x, devemos ter $a * x = 0$, uma vez que 0 é o elemento identidade, segundo a parte (c). Calcule como se segue:

$$a * x = 0, \quad a + x - ax = 0, \quad a = ax - x, \quad a = x(a - 1), \quad x = a/(a - 1)$$

Assim, se $a \neq 1$, então a possui um inverso que é $a/(a - 1)$.

B.2 Seja S um semigrupo com identidade e, e considere que b e b' são inversos de a. Mostre que $b = b'$, isto é, que inversos são únicos, se existirem.

Temos:

$$b * (a * b') = b * e = b \quad \text{e} \quad (b * a) * b' = e * b' = b'$$

Uma vez que S é associativo, $(b * a) * b' = b * (a * b')$; logo, $b = b'$.

B.3 Seja $S = \mathbf{N} \times \mathbf{N}$. Considere que $*$ é a operação em S definida por $(a, b) * (a', b') = (aa', bb')$.

(a) Mostre que $*$ é associativa. (Logo, S é um semigrupo.)

(b) Defina $f : (S, *) \to (\mathbf{Q}, \times)$ por meio de $f(a, b) = a/b$. Mostre que f é um homomorfismo.

(c) Encontre a relação de congruência $\sim$ em S determinada pelo homomorfismo f, isto é, onde $x \sim y$ se $f(x) = f(y)$. (Veja o Teorema B.4.)

(d) Descreva $S/\sim$. $S/\sim$ possui um elemento identidade? Ele possui inversos?

Suponha que $x = (a, b)$, $y = (c, d)$, $z = (e, f)$.

(a) Temos

$$\begin{aligned}(xy)z &= (ac, bd) * (e, f) = [(ac)e, (bd)f] \\ x(yz) &= (a, b) * (ce, df) = [a(ce), b(df)]\end{aligned}$$

Uma vez que a, b, c, d, e e f são inteiros positivos, $(ac)e = a(ce)$ e $(bd)f = b(df)$. Logo, $(xy)z = x(yz)$ e, portanto, é associativa. Isto é, $(S, *)$ é um semigrupo.

(b) f é um homomorfismo, uma vez que

$$f(x * y) = f(ac, bd) = (ac)/(bd) = (a/b)(c/d) = f(x)f(y)$$

(c) Suponha que $f(x) = f(y)$. Então $a/b = c/d$ e, portanto, $ad = bc$. Logo, f determina a relação de congruência $\sim$ em S, definida por $(a, b) \sim (c, d)$ se $ad = bc$.

(d) A imagem de f é $\mathbf{Q}^+$, o conjunto de números racionais positivos. Segundo o Teorema B.3, $S/\sim$ é isomorfo a $\mathbf{Q}^+$. Logo, $S/\sim$ possui um elemento identidade, e todo elemento possui um inverso.

B.4 Demonstre o Teorema B.1. Suponha que $*$ é uma operação associativa em um conjunto S. Então, qualquer produto $a_1 * a_2 * \ldots * a_n$ não precisa de parênteses, isto é, todos os produtos possíveis são iguais.

A demonstração é feita por meio de indução em n. Uma vez que n é associativa, o teorema é válido para $n = 1, 2$ e 3. Suponha que $n \geq 4$. Usamos a notação:

$$(a_1a_2 \cdots a_n) = (\cdots((a_1a_2)a_3)\cdots)a_n \quad \text{e} \quad [a_1a_2\cdots a_n] = \text{a qualquer produto}$$

Mostramos que $[a_1a_2\cdots a_n] = (a_1a_2 \cdots a_n)$ e, portanto, todos os produtos serão iguais. Uma vez que $[a_1a_2 \cdots a_n]$ denota algum produto, existe um $r < n$ tal que $[a_1a_2 \cdots a_n] = [a_1a_2 \cdots a_r][a_{r+1} \cdots a_n]$. Portanto, por indução,

$$\begin{aligned}[a_1a_2 \cdots a_n] &= [a_1a_2 \cdots a_r][a_{r+1} \cdots a_n] = [a_1a_2 \cdots a_r](a_{r+1} \cdots a_n)\\ &= [a_1 \cdots a_r]((a_{r+1} \cdots a_{n-1})a_n) = ([a_1 \cdots a_r](a_{r+1} \cdots a_{n-1}))a_n\\ &= [a_1 \cdots a_{n-1}]a_n = (a_1 \cdots a_{n-1})a_n = (a_1a_2 \cdots a_n)\end{aligned}$$

Logo, o teorema está demonstrado.

B.5 Demonstre o Teorema B.4. Seja $f: S \to S'$ um homomorfismo de semigrupos. Considere que $a \sim b$ se $f(a) = f(b)$. Então: (i) $\sim$ é uma relação de congruência; (ii) $S/\sim$ é isomorfo a $f(S)$.

(i) Em primeiro lugar, mostramos que $\sim$ é uma relação de equivalência. Uma vez que $f(a) = f(a)$, temos $a \sim a$. Se $a \sim b$, então $f(a) = f(b)$ ou $f(b) = f(a)$; logo, $b \sim a$. Por último, se $a \sim b$ e $b \sim c$, então $f(a) = f(b)$ e $f(b) = f(c)$, então, $f(a) = f(c)$. Logo, $a \sim c$. Isto é, $\sim$ é uma relação de equivalência. Suponha agora que $a \sim a'$ e $b \sim b'$. Então $f(a) = f(a')$ e $f(b) = f(b')$.

Uma vez que f é um homomorfismo,

$$f(ab) = f(a)f(b) = f(a')f(b') = f(a'b')$$

Portanto, $ab \sim a'b'$. Isto é, $\sim$ é uma relação de congruência.

(ii) Defina $\Psi: S/\sim \to f(S)$ por meio de $\Psi([a]) = f(a)$. Precisamos provar: (1) Ψ é bem definido, isto é, $\Psi([a]) \in f(S)$, e se $[a] = [b]$, então $f([a]) = f([b])$. (2) Ψ é um isomorfismo, isto é, Ψ é um homomorfismo, um para um e sobrejetor.

(1) *Prova de que Ψ é bem definido.* Temos $\Psi([a]) = f(a)$. Uma vez que $a \in S$, temos $f(a) \in f(S)$. Logo, $\Psi([a]) \in f(S)$, como pedido. Agora suponha que $[a] = [b]$. Então $a \sim b$ e, portanto, $f(a) = f(b)$. Logo,

$$\Psi([a]) = f(a) = f(b) = ([b])$$

Isto é, Ψ é bem definido.

(2) *Prova de que Ψ é um isomorfismo.* Uma vez que f é um homomorfismo,

$$\Psi([a][b]) = \Psi[ab] = f(ab) = f(a)f(b) = \Psi([a])\Psi([b])$$

Logo, Ψ é um homomorfismo. Suponha que $\Psi([a]) = \Psi([b])$. Então $f(a) = f(b)$ e, portanto, $a \sim b$. Logo, $[a] = [b]$ e Ψ é um para um. Por último, considere que $y \in f(S)$. Então, $(a) = y$ para algum $a \in S$. Portanto, $\Psi([a]) = f(a) = y$. Logo, Ψ é sobrejetora sobre $f(S)$. Consequentemente, Ψ é um isomorfismo.

Grupos

B.6 Considere o grupo $G = \{1, 2, 3, 4, 5, 6\}$ sob multiplicação módulo 7.

(a) Encontre a tabela de multiplicação de G. (b) Encontre $2^{-1}, 3^{-1}, 6^{-1}$.

(c) Encontre as ordens e os subgrupos gerados por 2 e 3. (d) G é cíclico?

(a) Para encontrar $a * b$ em G, encontre o resto quando o produto ab é dividido por 7.

Por exemplo, $5 \cdot 6 = 30$, que implica um resto de 2, quando dividido por 7, logo, $5 * 6 = 2$ em G. A tabela de multiplicação de G aparece na Fig. B-6(a).

(b) Note, em primeiro lugar, que 1 é o elemento identidade de G. Lembre-se de que a^{-1} é o elemento de G tal que $aa^{-1} = 1$. Logo, $2^{-1} = 4$, $3^{-1} = 5$ e $6^{-1} = 6$.

(c) Temos $2^1 = 2$, $2^2 = 4$, mas $2^3 = 1$. Logo, $|2| = 3$ e $gp(2) = \{1, 2, 4\}$. Temos $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. Portanto, $|3| = 6$ e $gp(3) = G$.

(d) G é cíclico, uma vez que $G = gp(3)$.

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(a)

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

(b)

Figura B-6

B.7 Seja G um sistema de resíduo reduzido módulo 15, digamos, $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (o conjunto de inteiros entre 1 e 15 que são coprimos a 15). Então, G é um grupo sob multiplicação módulo 15.

(a) Encontre a tabela de multiplicação de G.

(b) Encontre 2^{-1}, 7^{-1}, 11^{-1}.

(c) Encontre as ordens e os subgrupos gerados por 2, 7 e 11.

(d) G é cíclico?

(a) Para encontrar $a * b$ em G, encontre o restante quando o produto ab é dividido por 15. A tabela de multiplicação aparece na Fig. B-6(b).

(b) Os inteiros r e s são inversos se $r * s = 1$. Logo: $2^{-1} = 8$, $7^{-1} = 13$, $11^{-1} = 11$.

(c) Temos $2^2 = 4$, $2^3 = 8$, $2^4 = 1$. Logo, $|2| = 4$ e $gp(2) = \{1, 2, 4, 8\}$. Além disso, $7^2 = 4$, $7^3 = 4 * 7 = 13$, $7^4 = 13 * 7 = 1$. Então, $|7| = 4$ e $gp(7) = \{1, 4, 7, 13\}$. Por último, $11^2 = 1$. Portanto, $|11| = 2$ e $gp(11) = \{1, 11\}$.

(d) Não, uma vez que nenhum elemento gera G.

B.8 Considere o grupo simétrico S_3, cuja tabela de multiplicação é dada na Fig. B-4.

(a) Encontre a ordem e o grupo gerado para cada elemento de S_3.

(b) Encontre o número de todos os subgrupos de S_3.

(c) Sejam $A = \{\sigma_1, \sigma_2\}$ e $B = \{\phi_1, \phi_2\}$. Encontre AB, $\sigma_3 A$ e $A\sigma_3$.

(d) Sejam $H = gp(\sigma_1)$ e $K = gp(\sigma_2)$. Mostre que HK não é um subgrupo de S_3.

(e) S_3 é cíclico?

(a) Existem seis elementos: (1) ε, (2) σ_1, (3) σ_2, (4) σ_3, (5) ϕ_1, (6) ϕ_2. Encontre as potências de cada elemento x até que $x^n = \varepsilon$. Então $|x| = n$ e $gp(x) = \{\varepsilon, x^1, x^2, \ldots, x^{n-1}\}$. Note que $x^1 = x$, então precisamos apenas começar com $n = 2$, quando $x \neq \varepsilon$.

(1) $\varepsilon^1 = \varepsilon$; então $|\varepsilon| = 1$ e $g(\varepsilon) = \{\varepsilon\}$.

(2) $\sigma_1^2 = \varepsilon$; logo $|\sigma_1| = 2$ e $gp(\sigma_1) = \{\varepsilon, \sigma_1\}$.

(3) $\sigma_2^2 = \varepsilon$; logo $|\sigma_2| = 2$ e $gp(\sigma_2) = \{\varepsilon, \sigma_2\}$.

(4) $\sigma_3^2 = \varepsilon$; logo $|\sigma_3| = 2$ e $gp(\sigma_3) = \{\varepsilon, \sigma_3\}$

(5) $\phi_1^2 = \phi_2$, $\phi_1^3 = \phi_2\phi_1 = \varepsilon$; logo $|\phi_1| = 3$ e $gp(\phi_1) = \{\varepsilon, \phi_1, \phi_2\}$.

(6) $\phi_2^2 = \phi_1$, $\phi_2^3 = \phi_1\phi_2 = \varepsilon$; logo $|\phi_2| = 3$ e $gp(\phi_1) = \{\varepsilon, \phi_2, \phi_1\}$.

(b) Em primeiro lugar, $H_1 = \{\varepsilon\}$ e $H_2 = S_3$ são subgrupos de S_3. Qualquer outro subgrupo S_3 deve ter ordem 2 ou 3, uma vez que sua ordem deve dividir $|S_3| = 6$. Como 2 e 3 são números primos, esses subgrupos precisam ser

cíclicos (Problema B 61) e, portanto, devem aparecer na parte (a). Logo, os outros subgrupos de S_3 estão listados a seguir:

$$H_3 = \{\varepsilon, \sigma_1\}, \quad H_4 = \{\varepsilon, \sigma_2\}, \quad H_5 = \{\varepsilon, \sigma_3\}, \quad H_6 = \{\varepsilon, \phi_1, \phi_2\}$$

Então, S_3 possui seis subgrupos.

(*c*) Multiplique cada elemento de A por cada elemento em B:

$$\sigma_1\phi_1 = \sigma_2, \quad \sigma_1\phi_2 = \sigma_3, \quad \sigma_3\phi_1 = \sigma_3, \quad \sigma_2\phi_2 = \sigma_1$$

Logo, AB $= \{\sigma_1, \sigma_2, \sigma_3\}$

Multiplique σ_3 por cada elemento de A:

$$\sigma_3\sigma_1 = \phi_1, \sigma_3\sigma_2 = \phi_2, \text{ portanto, } \sigma_3 A = \{\phi_1, \phi_2\}$$

Multiplique cada elemento de A por σ_3

$$\sigma_1\sigma_3 = \phi_2, \quad \sigma_2\sigma_3 = \phi_1, \quad \text{portanto,} \quad A\sigma_3 = \{\phi_1, \phi_2\}$$

(*d*) $H = \{e, \sigma_1\}$, $K = \{e, \sigma_2\}$ e, então, $HK = \{e, \sigma_1, \sigma_2, \phi_1\}$, que não é um subgrupo de S_3, uma vez que HK possui quatro elementos.

(*e*) S_3 não é cíclico, uma vez que S_3 não é gerado por nenhum de seus elementos.

B.9 Sejam σ e τ os seguintes elementos do grupo simétrico S_6.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} \text{ e } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$$

Encontre: $\tau\sigma$, $\sigma\tau$, σ^2 e σ^{-1}. (Uma vez que σ e τ são funções, $\tau\sigma$ significa aplicar σ e, então, τ.)

A Figura B-7 mostra os efeitos sob 1, 2, . . . , 6 da composição de permutações:

(*a*) σ e, então, τ; (*b*) τ e, então, σ; (c) σ e, então, σ, ou seja, σ^2.

Portanto:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 4 & 3 \end{pmatrix} \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix} \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix}$$

Obtemos σ^{-1} por meio da permutação das linhas superiores e inferiores e, então, rearranjamos.

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 5 & 4 & 6 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$$

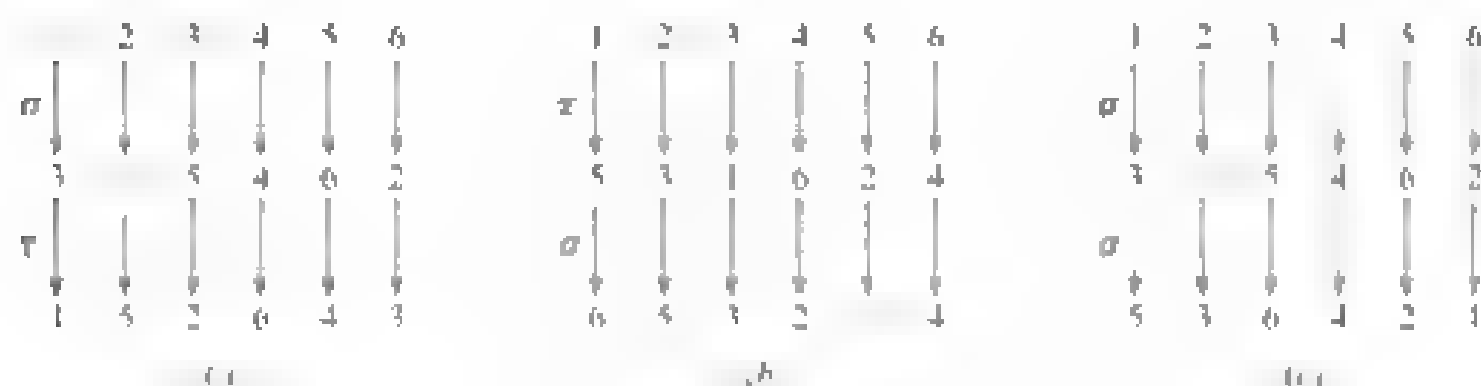



Figura B-7

B.10 Sejam H e K dois grupos.

(*a*) Defina o produto direto $G = H \times K$ de H e K.

(*b*) Qual é o elemento identidade e a ordem de $G = H \times K$?

(*c*) Descreva e encontre a tabela de multiplicação do grupo $G = \mathbf{Z}_2 \times \mathbf{Z}_2$.

(*a*) Seja $G = H \times K$, o produto cartesiano de H e K, com a operação $*$ definida em relação aos componentes por meio de

$$(h, k) * (h', k') = (hh', kk')$$

Então, G é um grupo (Problema B.68), chamado de *produto direto* de H e K

(*b*) O elemento $e = (e_H, e_K)$ é o elemento identidade de G, e $|G| = |H| \cdot |K|$

(*c*) Uma vez que $\mathbf{Z}_2$ possui dois elementos, G possui quatro. Considere que

$$e = (0, 0), \quad a = (1, 0), \quad b = (0, 1), \quad c = (1, 1)$$

A tabela de multiplicação de G aparece na Fig B-8(*a*). Note que G é abeliano, uma vez que a tabela é simétrica. Além disso, $a^2 = e$, $b^2 = e$ e $c^2 = e$. Logo, G não é cíclico e, portanto, $G \ncong \mathbf{Z}_4$.

B.11 Seja S o quadrado no plano $\mathbf{R}^2$ esboçado na Fig. B-8(*b*), com seu centro na origem 0. Note que os vértices de S são enumerados no sentido anti-horário de 1 até 4

(*a*) Defina o grupo G de simetrias de S.

(*b*) Liste os elementos de G.

(*c*) Encontre um conjunto mínimo de geradores de G.

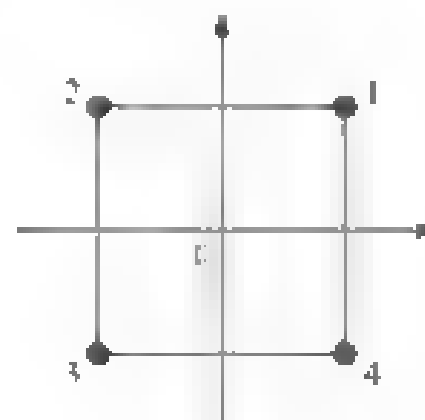



Figura B-8

(*a*) Uma simetria σ de S é uma correspondência rígida de um para um entre S e ele mesmo. (Aqui, rígido significa que as distâncias entre os pontos não muda.) O grupo G de simetrias de S é o conjunto de todas as simetrias de S sob composição de mapeamentos.

(*b*) Existem oito simetrias como se segue. Para $\alpha = 0°, 90°, 180°, 270°$, considere que $\sigma(\alpha)$ é a simetria obtida pela rotação de S pelo seu centro α graus e que $\tau(\alpha)$ é a simetria obtida pela reflexão de S sobre o eixo y e, então, girando S em torno de seu próprio centro α graus. Note que qualquer simetria σ de S é completamente determinada pelo seu efeito nos vértices de S e, portanto, σ pode ser representado como uma permutação em S_4. Logo:

$$\sigma(0°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma(90°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$\sigma(180°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 4 \end{pmatrix}, \quad \sigma(270°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\tau(0°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \tau(90°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\tau(180°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \tau(270°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

(*c*) Considere que $a = \sigma(90°)$ e $b = \tau(0°)$. Então a e b formam um conjunto máximo de geradores de G. Especificamente,

$$\sigma(0°) = a^4, \quad \sigma(90°) = a, \quad \sigma(180°) = a^2, \quad \sigma(270°) = a^3$$

$$\tau(0°) = b, \quad \tau(90°) = ba, \quad \tau(180°) = ba^2, \quad \tau(270°) = ba^3$$

e G não é cíclico, então ele não é gerado por um elemento. (É possível mostrar que as relações $a^4 = e$, $b^2 = e$ e $bab = a^{-1}$ descrevem completamente G.)

B.12 Seja G um grupo e A um conjunto não vazio.

(a) Defina o significado da afirmação "G age sobre A".

(b) Defina o estabilizador H_a de um elemento $a \in A$.

(c) Mostre que H_a é um subgrupo de G.

(a) Considere que PERM(A) denota o grupo de todas as permutações de A. Seja $\psi: G \to \text{PERM}(A)$ qualquer homomorfismo. Então G é considerado como agindo sobre A, onde cada elemento g em G define uma permutação $g: A \to A$ por meio de

$$g(a) = (\psi(g))(a)$$

(Frequentemente, a permutação $g: A \to A$ é dada diretamente e, logo, o homomorfismo é definido implicitamente.)

(b) O estabilizador H_a de $a \in A$ consiste em todos os elementos de G que "fixam a", isto é,

$$H_a = \{g \in G \mid g(a) = a\}$$

(c) Uma vez que $e(a) = a$, temos $e \in H_a$. Suponha que $g, g' \in H_a$. Então, $(gg')(a) = g(g'(a)) = g(a) = a$, logo, $gg' \in H_a$. Além disso, $g^{-1}(a) = a$, uma vez que $g(a) = a$, então, $g^{-1} \in H_a$. Portanto, H_a é um subgrupo de G.

B.13 Demonstre o Teorema B.6: Considere que H é um subgrupo de um grupo G. Então os co-conjuntos à direita Ha formam uma partição de G.

Uma vez que $e \in H$, temos $a = ea \in H_a$, logo, todo elemento pertence a um co-conjunto. Agora suponha que Ha e Hb não são disjuntos. Digamos $c \in Ha \cap Hb$. A demonstração estará completa se mostrarmos que $Ha = Hb$.

Uma vez que c pertence tanto a Ha quanto a Hb, temos $c = h_1a$ e $c = h_2b$, onde $h_1, h_2 \in H$. Então $h_1a = h_2b$ e, portanto, $a = h_1^{-1}h_2b$. Seja $x \in Ha$. Então

$$x = h_3a = h_3h_1^{-1}h_2b$$

onde $h_3 \in H$. Uma vez que H é um subgrupo $h_3h_1^{-1}h_2 \in H$, portanto, $x \in Hb$. Uma vez que x era qualquer elemento de Ha, temos $Ha \subset Hb$. De forma similar, $Hb \subset Ha$. Ambas as inclusões implicam $Ha = Hb$, e o teorema está demonstrado.

B.14 Seja H um subgrupo finito de G. Mostre que H e qualquer co-conjunto Ha possui o mesmo número de elementos.

Seja $H = \{h_1, h_2, \ldots, h_k\}$, onde H possui k elementos. Então $Ha = \{h_1a, h_2a, \ldots, h_ka\}$.

Contudo, $h_ia = h_ja$ implica $h_i = h_j$; logo, os k elementos listados em Ha são distintos. Portanto, H e Ha possuem o mesmo número de elementos.

B.15 Demonstre o Teorema B.7 (Lagrange): Seja H um subgrupo de um grupo finito G. Então a ordem de H divide a ordem de G.

Suponha que H possui r elementos e existem co-conjuntos à direita s; digamos,

$$Ha_1, Ha_2, \ldots, Ha_s$$

Segundo o Teorema B.6, a partição G de co-conjuntos e o Problema B.14, cada co-conjunto possui r elementos. Logo, G possui rs elementos e, portanto, a ordem de H divide a ordem de G.

B.16 Prove: Todo subgrupo de um grupo cíclico G é também cíclico.

Uma vez que G é cílico, existe um elemento $a \in G$ tal que $G = gp(a)$. Seja H um subgrupo de G. Se $H = \{e\}$, então $H = gp(e)$ e H é cíclico. Caso contrário, H contém uma potência diferente de zero de a. Uma vez que H é um subgrupo, ele deve ser fechado sob inversos e, portanto, H contém potências positivas de a. Seja m a menor potência positiva de a, tal que a^m pertence a H. Dizemos que $b = a^m$ gera H. Seja x qualquer outro elemento de H; desde que x pertença a G, temos $x = a^n$ para qualquer inteiro n. Dividindo n por m, temos um quociente q e um resto r, isto é,

$$n = mq + r$$

onde $0 < r < m$. Então

$$a^n = a^{mq+r} = a^{mq} \cdot a^r = b^q \cdot a^r, \quad \text{de modo que} \quad a^r = b^{-q}a^n$$

Mas a^n e $b \in H$. Uma vez que H é um subgrupo, $b^{-q}a^n \in H$, o que significa que $a^r \in H$. Contudo, m é a menor potência positiva de um elemento pertencente a H. Portanto, $r = 0$. Logo, $x = a^n = b^q$. Então, b gera H, e H é cíclico.

B.17 Demonstre o Teorema B.8. Seja H um subgrupo normal de um grupo G. Então os co-conjuntos de H formam um grupo sobre multiplicação de co-conjuntos definido por $(aH)(bH) = abH$.

Multiplicação de co-conjuntos é bem definida, uma vez que

$$(aH)(bH) = a(Hb)H = a(bH)H = ab(HH) = abH$$

(Aqui, usamos o fato de que H é normal, então $Hb = bH$ e, segundo o Problema B.57, $HH = H$.) Associatividade de multiplicação de co-conjuntos é consequência do fato de que essa propriedade é válida em G. H é o elemento identidade de G/H, uma vez que

$$(aH)H = a(HH) = aH \text{ e } H(aH) = (Ha)H = (aH)H = aH$$

Por último, $a^{-1}H$ é o inverso de aH, uma vez que

$$(a^{-1}H)(aH) = a^{-1}aHH = eH = H \text{ e } (aH)(a^{-1}H) = aa^{-1}HH = eH = H$$

Logo, G/H é um grupo fechado sob multiplicação de co-conjuntos.

B.18 Suponha que $F: G \to G'$ é um homomorfismo de grupos. Prove: (a) $f(e) = e'$; (b) $(fa^{-6}) = f(a)^{-1}$

(*a*) Uma vez que $e = ee$ e f é um homomorfismo, temos

$$f(e) = f(ee) = f(e)f(e)$$

Multiplicando ambos os lados por $f(e)^{-1}$, temos o nosso resultado.

(*b*) Usando a parte (a) e o fato de que $aa^{-1} = a^{-1}a = e$, temos

$$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) \quad \text{e} \quad e' = f(e) = f(a^{-1}a) = f(a^{-1})f(a)$$

Uma vez que $f(a^{-1})$ é o inverso de $f(a)$, isto é, $f(a^{-1}) = (f(a))^{-1}$.

B.19 Demonstre o Teorema B.9: Seja $f: G \to G'$ um homomorfismo com núcleo K, então K é um subgrupo normal de G, e G/K é isomorfo à imagem de g. (Compare com o Problema B.5, o teorema análogo para semigrupos.)

Prova de que K é normal: Segundo o Problema B.18, $f(e) = e'$, então $e \in K$. Agora suponha que $a, b \in K$ e $g \in G$. Então, $f(a) = e'$ e $f(b) = e'$. Logo,

$$f(ab) = f(a)f(b) = e'e' = e'$$
$$f(a^{-1}) = f(a)^{-1} = e'^{-1} = e'$$
$$f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)e'f(g)^{-1} = e'$$

Logo, ab, a^{-1} e gag^{-1} pertencem a K, então K é um subgrupo normal.

Prova de que $G/K \cong H$, onde H é a imagem de f. Seja $\varphi: G/K \to H$ definido por

$$\varphi(Ka) = f(a)$$

Mostramos que φ é bem definido, ou seja, se $Ka = Kb$, então $\varphi(Ka) = \varphi(Kb)$. Suponha que $Ka = Kb$. Então $ab^{-1} \in K$ (Problema B.57). Logo, $f(ab^{-1}) = e'$ e, portanto,

$$f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) = e'$$

Logo, $f(a) = f(b)$ e, portanto, $\varphi(Ka) = \varphi(Kb)$. Então φ é bem definido.

Mostramos a seguir que φ é um homomorfismo:

$$\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb)$$

Logo, φ é um homomorfismo. Mostramos a seguir que φ é um para um. Suponha que $\varphi(Ka) = \varphi(Kb)$. Então

$$f(a) = f(b) \quad \text{ou} \quad f(a)f(b)^{-1} = e' \quad \text{ou} \quad f(a)f(b^{-1}) = e' \quad \text{ou} \quad f(ab^{-1}) = e'$$

Logo, $ab^{-1} \in K$ e, segundo o Problema B.57, temos $Ka = Kb$. Então, φ é um para um. A seguir, mostramos que φ é sobrejetora. Seja $h \in H$. Uma vez que H é a imagem de f, existe um $a \in G$ tal que $f(a) = h$. Logo, $\varphi(Ka) = f(a) = h$, de modo que φ é sobrejetora. Consequentemente, $G/K \cong H$ e o teorema está provado.

Anéis, domínios de integridade e corpos

B.20 Considere o anel $\mathbf{Z}_{10} = \{0, 1, 2, \ldots, 9\}$ de inteiros módulo 10. (*a*) Encontre as unidades de $\mathbf{Z}_{10}$. (*b*) Encontre -3, -8 e 3^{-1}. (*c*) Considere que $f(x) = 2x^2 + 4x + 4$. Encontre as raízes de $f(x)$ sobre $\mathbf{Z}_{10}$.

(*a*) Segundo o Problema B.78, os inteiros relativamente primos ao módulo $m = 10$ são as unidades em $\mathbf{Z}_{10}$. Logo, as unidades são 1, 3, 7 e 9.

(*b*) Lembre-se de que $-a$ em um anel R é o elemento que $a+(-a) = (-a)+a = 0$. Logo, $-3 = 7$, uma vez que $3+7 = 7+3 = 0$ em $\mathbf{Z}_{10}$. De forma similar, $-8 = 2$. Lembre-se de que a^{-1} em um anel R é o elemento que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Logo, $3^{-1} = 7$, uma vez que $3 \cdot 7 = 7 \cdot 3 = 1$ em $\mathbf{Z}_{10}$.

(*c*) Substitua cada um dos dez elementos de $\mathbf{Z}_{10}$ em $f(x)$ para ver quais elementos levam a 0. Temos,

$$f(0) = 4, \quad f(2) = 0, \quad f(4) = 2, \quad f(6) = 0, \quad f(8) = 4$$
$$f(1) = 0, \quad f(3) = 4, \quad f(5) = 4, \quad f(7) = 0, \quad f(9) = 2$$

Logo, as raízes são 1, 2, 6 e 7. (Este exemplo mostra que um polinômio de grau n pode ter mais do que n raízes sobre um anel arbitrário. Isso não pode acontecer se o anel é em um corpo.)

B.21 Prove que, em um anel R: (i) $a \cdot 0 = 0 \cdot a = 0$, (ii) $a(-b) = (-a)b = -ab$, (iii) $(-1)a = -a$ (quando R possui um elemento identidade 1).

(i) Uma vez que $0 = 0 + 0$, temos

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$$

Somando $-(a \cdot 0)$ a ambos os lados, implica $0 = a \cdot 0$. De forma similar, $0 \cdot a = 0$.

(ii) Usando $b + (-b) = (-b) + b = 0$, temos

$$ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$$
$$a(-b) + ab = a((-b) + b) = a \cdot 0 = 0$$

Logo, $a(-b)$ é o negativo de ab; isto é, $a(-b) = -ab$. De forma similar, $(-a)b = -ab$.

(iii) Temos

$$a + (-1)a = 1 \cdot a + (-1)a = (1 + (-1))a = 0 \cdot a = 0$$
$$(-1)a + a = (-1)a + 1 \cdot a = ((-1) + 1)a = 0 \cdot a = 0$$

Logo, $(-1)a$ é o negativo de a; isto é, $(-1)a = -a$.

B.22 Seja D um domínio de integridade. Mostre que se $ab = ac$ com $a \neq 0$, então $b = c$.

Uma vez que $ab = ac$, temos

$$ab - ac = 0 \quad \text{e, portanto,} \quad a(b - c) = 0$$

Uma vez que $a \neq 0$, devemos ter $b - c = 0$, já que D não possui divisores zero. Logo, $b = c$.

B.23 Suponha que J e K são ideais em um anel R. Mostre que $J \cap K$ é um ideal em R.

Uma vez que J e K são ideais, $0 \in J$ e $0 \in K$. Logo, $0 \in J \cap K$. Agora considere que $a, b \in J \cap K$ e assuma que $r \in R$. Então $a, b \in J$ e $a, b \in K$. Uma vez que J e K são ideais,

$$a - b,\ ra,\ ar \in J \quad \text{e} \quad a - b,\ ra,\ ar \in K$$

Então $a - b$, ra, $ar \in J \cap K$. Portanto, $J \cap K$ é um ideal.

B.24 Seja J um ideal em um anel R com elemento identidade 1. Prove: (*a*) Se $1 \in J$, então $J = R$; (*b*) Se qualquer unidade $u \in J$, então $J = R$.

(*a*) Se $1 \in J$, então para qualquer $r \in R$, temos $r \cdot 1 \in R$ ou $r \in J$. Logo, $J = R$.

(*b*) Se $u \in J$, então $u^{-1} \cdot u \in J$ ou $1 \in J$. Logo, $J = R$, segundo a parte (a).

B.25 Prove. (*a*) Um domínio de integridade finito D é um corpo. (*b*) $\mathbf{Z_p}$ é um corpo onde p é um número primo. (*c*) (Fermat) Se p é primo, então $a^p \equiv a \pmod{p}$ para qualquer inteiro a.

(*a*) Suponha que D possui n elementos, digamos $D = \{a_1, a_2, \ldots, a_n\}$. Seja a qualquer elemento diferente de zero de D. Considere os n elementos

$$aa_1, aa_2, \ldots, a_n$$

Uma vez que $a \neq 0$, temos $aa_i = aa_k$ que implica $a_i = a_k$ (Problema B.22). Logo, os n elementos acima são distintos e, portanto, eles devem ser um novo arranjo dos elementos de D. Um deles, digamos aa_k deve ser igual ao elemento identidade 1 de D; isto é, $aa_k = 1$. Logo, a_k é o inverso de a. Uma vez que a é qualquer elemento diferente de zero de D, temos D como um corpo.

(*b*) Lembre-se de que $\mathbf{Z_p} = \{0, 1, 2, \ldots, p - 1\}$. Mostramos que $\mathbf{Z_p}$ não possui divisores zero. Suponha que $a * b = 0$ em $\mathbf{Z_p}$, isto é, $0 \pmod{p}$. Então p divide ab. Uma vez que p é primo, ele divide a ou b. Então $a \equiv 0 \pmod{p}$ ou $b \equiv 0 \pmod{p}$, isto é, $a = 0$ ou $b = 0$ em $\mathbf{Z_p}$. Consequentemente, $\mathbf{Z_p}$ não possui divisores zero e, portanto, $\mathbf{Z_p}$ é um domínio de integridade. Segundo a parte (a), $\mathbf{Z_p}$ é um corpo.

(*c*) Se p divide a, então $a \equiv 0 \pmod{p}$ e, portanto, $a^p \equiv a \equiv 0 \pmod{p}$. Suponha que p não divide a, então a pode ser visto como um elemento diferente de zero de $\mathbf{Z_p}$, seus elementos diferentes de zero formam um grupo G sob multiplicação de ordem $p - 1$. Segundo o Problema B.45, $a^{p-1} = 1$ em $\mathbf{Z_p}$.

Em outras palavras, $a^{p-1} \equiv 1 \pmod{p}$. Multiplicação por a nos dá $a^p \equiv a \pmod{p}$ e o teorema está provado.

Polinômios sobre um corpo

B.26 Suponha que $f(t) = 2t^3 - 3t^2 - 6t - 2$. Encontre todas as raízes de $f(t)$, sabendo que $f(t)$ possui uma raiz racional.

As raízes racionais de $f(t)$ devem estar entre ± 1, ± 2 e $\pm 1/2$. Testando cada raiz possível, temos, pela divisão sintética (ou dividindo por $2t + 1$),

$$\begin{array}{r|rrrr} -\frac{1}{2} & 2 & -3 & -6 & -2 \\ & & -1 & +2 & +2 \\ \hline & 2 & -4 & -4 & +0 \end{array}$$

Portanto, $t = -1/2$ é uma raiz e

$$f(t) = (t + 1/2)(2t^2 - 4t - 4) = (2t + 1)(t^2 - 2t - 2)$$

Agora podemos usar a fórmula quadrática em $t^2 - 2t - 2$ para obter as três raízes a seguir de $f(t)$.

$$t = -1/2, \quad t = 1 + \sqrt{3}, \quad t = 1 - \sqrt{3}$$

B.27 Seja $f(t) = t^4 - 3t^3 + 3t^2 + 3t - 20$. Encontre todas as raízes de $f(t)$, considerando que $t = 1 + 2i$ é uma raiz.

Uma vez que $1 + 2i$ é uma raiz, então $1 - 2i$ á uma raiz e $c(t) = t^2 - 2t + 5$ é um fator de $f(t)$. Dividindo $f(t)$ por $c(t)$, temos

$$f(t) = (t^2 - 2t + 5)(t^2 - t - 4)$$

A fórmula quadrática com $t^2 - t - 4$ nos dá as outras raízes de $f(t)$. Isto é, as quatro raízes de $f(t)$ são as seguintes

$$t = 1 + 2i, \quad t = 1 - 2i, \quad t = (1 + \sqrt{17})/2, \quad t = (1 - \sqrt{17})/2$$

B.28 Seja $K = \mathbf{Z_8}$. Encontre todas as raízes de $f(t) = t^2 + 6t$.

Aqui, $\mathbf{Z_8} = \{0, 1, 2, \ldots, 7\}$. Substitua cada elemento de $\mathbf{Z_8}$ em $f(t)$ para obter:

$$f(0) = 0, \quad f(2) = 0, \quad f(4) = 0, \quad f(6) = 0$$

Então $f(t)$ possui quatro raízes, $t = 0, 2, 4, 6$. (O Teorema B.21 não é válido aqui, uma vez que K não é um corpo).

B.29 Suponha que $f(t)$ é um polinômio real com grau n ímpar. Mostre que $f(t)$ possui uma raiz real.

As raízes complexas (não reais) vêm em pares. Uma vez que $f(t)$ possui um número ímpar n de raízes (contando multiplicidade), $f(t)$ deve possuir pelo menos uma raiz real.

B.30 Demonstre o Teorema B.15 (Algoritmo de divisão euclidiana): Sejam $f(t)$ e $g(t)$ polinômios sobre um corpo K com $g(t) \neq 0$. Então existem polinômios $q(t)$ e $r(t)$ tal que

$$f(t) = q(t)g(t) + r(t)$$

onde $r(t) \equiv 0$ ou $\deg(r) < \deg(g)$.

Se $f(t) = 0$ ou $\deg(f) < \deg(g)$, então temos a representação necessária $f(t) = 0g(t) + f(t)$. Agora suponha que $\deg(f) \geq \deg(g)$, digamos

$$f(t) = a_nt^n + \cdots + a_1t + a_0 \quad \text{e} \quad g(t) = b_mt^m + \cdots + b_1t + b_0$$

onde $a_n, b_m \neq 0$ e $n > m$. Formamos o polinômio

$$f_1(t) = f(t) - \frac{a_n}{b_m}t^{n-m}g(t)$$

(Este é o primeiro passo de subtração em "divisão longa".) Então $\deg(f_1) < \deg(f)$. Por indução, existem polinômios $q_1(t)$ e $r(t)$ tal que $f_1(t) = q_1(t)g(t) + r(t)$, onde $r(t) \equiv 0$ ou $\deg(r) < \deg(g)$. Substituindo isso em (1) e resolvendo para $f(t)$, temos

$$f(t) = \left[q_1(t) + \frac{a_n}{b_m}t^{n-m}\right]g(t) + r(t)$$

que é a representação desejada.

B.31 Demonstre o Teorema B.18. Suponha que $f(t)$ é um polinômio sobre um corpo K e $\deg(f) = n$. Então $f(t)$ possui, no máximo, n raízes.

A demonstração é feita por indução em n. Se $n = 1$, então $f(t) = at + b$ e $f(t)$ possui a raiz única $t = -b/a$. Suponha que $n > 1$. Se $f(t)$ não possui raízes, então o teorema é verdadeiro. Suponha que $a \in K$ é uma raiz de $f(t)$. Então

$$f(t) = (t - a)g(t) \tag{1}$$

onde $\deg(g) = n - 1$. Dizemos que qualquer outra raiz de $f(t)$ deve ser também uma raiz de $g(t)$.

Suponha que $b \neq a$ é outra raiz de $f(t)$. Substituindo $t = b$ em (1) implica $0 = f(b) = (b - a)g(b)$.

Uma vez que K não possui divisores zero e $b - a \neq 0$, devemos ter $g(b) = 0$. Por indução, $g(t)$ possui, no máximo, $n - 1$ raízes. Logo, $f(t)$ possui, no máximo, $n - 1$ raízes além de a. Então, $f(t)$ possui, no máximo, n raízes.

B.32 Demonstre o Teorema B.19. Suponha que um número racional p/q (reduzido aos menores termos) é uma raiz de um polinômio

$$f(t) = a_nt^n + \quad \cdot + a_1t + a_0$$

onde todos os coeficientes $a_n, \ldots, a_1, a_0$ são inteiros. Então p divide o termo constante a_0 e q divide o coeficiente principal a_n. Em particular, se $c = p/q$ é um inteiro, então c divide o termo constante a_0.

Substitua $t = p/q$ em $f(t) = 0$ para obter $a_n(p/q)^n + \quad + a_1(p/q) + a_0 = 0$. Multiplique ambos os lados da equação para obter

$$a_np^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \cdots + a_1pq^{n-1} + a_0q^n = 0 \tag{1}$$

Uma vez que p divide todos os n primeiros termos de (1), p deve dividir o último termo a_0q^n. Assumindo que p e q são relativamente primos, q divide a_0. De forma similar, q divide os n últimos termos de (1), portanto q divide o primeiro termo a_np^n. Uma vez que p e q são relativamente primos, q divide a_n.

B.33 Demonstre o Teorema B.20: O anel $K[t]$ de polinômios sobre um corpo K é um domínio ideal principal (DIP). Se J é um ideal em $K[t]$, então existe um polinômio mônico único d que gera J, isto é, todo polinômio f em J é um múltiplo de d.

Seja d um polinômio de menor grau em J. Uma vez que possamos multiplicar d por um escalar diferente de zero e ainda continuarmos com J, podemos assumir sem perda de generalidade que d é um polinômio mônico (com coeficiente principal igual a 1). Agora suponha que $f \in J$. Pela divisão algorítmica, existem polinômios q e r tal que $f = qd + r$ quando $r = 0$ ou $\deg(r) < \deg(d)$. Agora $f, d \in J$ implica $qd \in J$ e, portanto, $r = f - qd \in J$. Mas d é um polinômio de menor grau em J. Consequentemente, $r = 0$ e $f = qd$, isto é, d divide f. Ainda falta mostrar que d é único. Se d' é outro polinômio mônico que gera J, então d divide d' e d' divide d. Isso implica que $d = d'$, pois d e d' são mônicos. Logo, o teorema está provado.

B.34 Demonstre o Teorema B.21: Sejam f e g polinômios em $K[t]$, sendo que não são ambos o polinômio zero. Então existe um único polinômio mônico d tal que: (i) d divide tanto f quanto g. (ii) Se d' divide f e g, então d' divide d.

O conjunto $I = \{mf + ng \mid m, n \in K[t]\}$ é um ideal. Seja d o polinômio mônico que gera I. Note que $f, g \in I$, logo, d divide f e g. Agora suponha que d' divide f e g. Seja J o ideal gerado por d'. Então $f, g \in J$ e, portanto, $I \subseteq J$. Consequentemente, $d \in J$ e, portanto, d' divide d como foi dito. Ainda falta mostrar que d é único. Se d_1 é outro máximo divisor comum (mônico) de f e g, então d divide d_1 e d_1 divide d. Isso implica o fato de que $d = d_1$, pois d e d_1 são mônicos. Logo, o teorema está provado.

B.35 Demonstre o Corolário B.22. Seja d o máximo divisor comum de f e g. Então existem polinômios m e n tal que $d = mf + ng$. Em particular, se f e g são relativamente primos, então existem polinômios m e n tal que $mf + ng = 1$.

A partir do Teorema B.21, no Problema B.34, o máximo divisor comum d gera o ideal $I = \{mf + ng \mid m, n \in K[t]\}$. Logo, existem polinômios m e n tal que $d = mf + ng$.

B.36 Demonstre o Lema B.23. Suponha que $p \in K[t]$ é irredutível. Se p divide o produto fg de polinômios $f, g \in K[t]$, então p divide f ou p divide g. De forma mais geral, se p divide o produto $f_1f_2 \ldots f_n$ em n polinômios, então p divide um deles.

Suponha que p divide fg, mas não f. Uma vez que p é irredutível, os polinômios f e p devem, então, ser relativamente primos. Logo, existem polinômios $m, n \in K[t]$ tais que $mf + np = 1$. Multiplicando essa equação por g, obtemos $mfg + npg = g$. Mas p divide fg, e, portanto, p divide também mfg. Além disso, p divide npg. Portanto, p divide a soma $g = mfg + npg$.

Agora suponha que p divide $f_1f_2 \ldots f_n$. Se p divide f_1, então encerramos a questão. Caso contrário, considerando o resultado acima, p divide o produto $f_2 \ldots f_n$. Por indução em n, p divide um dos polinômios no produto $f_2 \ldots f_n$. Logo, o lema está provado.

B.37 Demonstre o Teorema B.24 (Teorema de fatoração única): Seja f um polinômio diferente de zero em $K[t]$. Então f pode ser escrito unicamente (exceto pela sua ordem) como um produto $f = kp_1p_2 \cdots p_n$, onde $k \in K$ e os p's são polinômios mônicos irredutíveis em $K[t]$.

Provemos, em primeiro lugar, a existência de tal produto. Se f é irredutível ou se $f \in K$, então tal produto claramente existe. Por outro lado, suponha que $f = gh$ onde g e h são não escalares. Então g e h possuem graus menores do que o de f. Por indução, podemos assumir que $g = k_1g_1g_2 \ldots g_r$ e $h = k_2h_1h_2 \ldots h_s$, onde $k_1, k_2 \in K$ e g_i e h_j são polinômios mônicos irredutíveis. Assim, nossa representação desejada é a que se segue

$$f = (k_1k_2)g_1g_2 \cdots g_rh_1h_2 \cdots h_s$$

A seguir, provamos unicidade (exceto pela ordem) de tal produto para f. Suponha que

$$f = kp_1p_2 \ldots p_n = k'q_1q_2 \ldots q_m \quad \text{onde} \quad k, k' \in K$$

e $p_1, \ldots, p_n, q_1, \ldots, q_m$ são polinômios mônicos irredutíveis. Agora p_1 divide $k'q_1 \ldots q_m$. Uma vez que p_1 é irredutível, ele deve didividr um dos q's, considerando o lema B.23. Digamos que p_1 divida q_1. Uma vez que p_1 e q_1 são irredutíveis e mônicos, $p_1 = q_1$. Consequentemente, $kp_2 \ldots p_n = k'q_2 \ldots q_m$. Por indução, temos que $n = m$ e $p_2 = q_2, \ldots, p_n = q_m$ para algum novo arranjo dos q's. Temos, também, que $k = k'$. Logo, o teorema está demonstrado.

B.38 Demonstre o Teorema B.25: Suponha que $f(t)$ é um polinômio sobre o corpo real R, e suponha que o número complexo $z = a + bi$, $b \neq 0$, é uma raiz de $f(t)$. Então, o conjugado complexo $\bar{z} = a - bi$ é também uma raiz de $f(t)$. Logo, a seguir, está um fator de $f(t)$:

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

Dividindo $f(t)$ por $c(t)$ onde $\deg(c) = 2$, existe um $q(t)$ e números reais M e N tal que

$$f(t) = c(t)q(t) + Mt + N \qquad (1)$$

Uma vez que $z = a + bi$ é uma raiz de $f(t)$ e $c(t)$, temos, por substituição, $t = a + bi$ em (1),

$$f(z) = c(z)q(z) + M(z) + n \quad \text{ou} \quad 0 = 0q(z) + M(z) + N \quad \text{ou} \quad M(a + bi) + N = 0$$

Logo, $Ma + N = 0$ e $Mb = 0$. Uma vez que $b \neq 0$, devemos ter $M = 0$. Então $0 + N = 0$ ou $N = 0$. Logo, $f(t) = c(t)q(t)$ e $\bar{z} = a - bi$ é uma raiz de $f(t)$.

Problemas Complementares

Operações e semigrupos

B.39 Considere o conjunto **N** de inteiros positivos, e considere que $*$ denota a operação que é o mínimo múltiplo comum (mmc) em N.

(a) Encontre $4 * 6$, $3 * 5$, $9 * 18$, $1 * 6$.

(b) $(\mathbf{N}, *)$ é um semigrupo? Ele é comutativo?

(c) Encontre o elemento identidade de $*$.

(d) Quais elementos em N, se existirem, possuem inversos, e quais são eles?

B.40 Seja $*$ a operação no conjunto **R** de números reais definida por $a * b = a + b + 2ab$.

(a) Encontre $2 * 3$, $3 * (-5)$ e $7 * (1/2)$. (b) $(\mathbf{R}, *)$ é um semigrupo? Ele é comutativo?

(c) Encontre o elemento identidade de $*$ (d) Quais elementos possuem inversos, e quais são eles?

B.41 Seja A um conjunto não vazio com a operação $*$ definida por $a * b = a$, e assuma que A possui mais de um elemento.

(a) A é um semigrupo? (c) A possui um elemento identidade?

(b) A é comutativo? (d) Quais elementos, se existirem, possuem inversos, e quais são eles?

B.42 Seja $A = \{a, b\}$ (a) Encontre o número de operações em A. (b) Aponte uma operação que não seja associativa nem comutativa.

B.43 Para cada um dos conjuntos a seguir, aponte quais são fechados sob (a) multiplicação, (b) adição.

$$A = \{0, 1\}, \quad B = \{1, 2\}, \quad C = \{x \mid x \text{ é primo}\}, D = \{2, 4, 8, \ldots\} = \{x \mid x = 2^n\}$$

B.44 Sejam $A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$, os múltiplos de 3. A é fechado sob.

(a) adição; (b) multiplicação; (c) subtração; (d) divisão (exceto por 0)

B.45 Encontre um conjunto A de três inteiros que seja fechado sob (a) multiplicação, (b) adição

B.46 Seja S um conjunto infinito. Seja A a coleção de subconjuntos finitos de S, e considere que B é a coleção de subconjuntos infinitos de S.

(a) A é fechado sob: (i) união; (ii) interseção; (iii) complementar?

(b) B é fechado sob: (i) união; (ii) interseção; (iii) complementar?

B.47 Seja $S = \mathbf{Q} \times \mathbf{Q}$ o conjunto de pares ordenados de números racionais, com a operação $*$ definida por

$$(a, b) * (x, y) = (ax, ay + b)$$

(a) Encontre $(3, 4) * (1, 2)$ e $(-1, 3) * (5, 2)$.

(b) S é um semigrupo? Ele é comutativo?

(c) Encontre o elemento identidade de S.

(d) Quais elementos, se existirem, possuem inversos, e quais são eles?

B.48 Seja $S = N \times N$ o conjunto de pares ordenados de inteiros positivos, com a operação $*$ definida por

$$(a, b) * (c, d) = (ad + bc, bd)$$

(a) Encontre $(3, 4) * (1, 5)$ e $(2, 1) * (4, 7)$.

(b) Mostre que $*$ é associativa. (Logo, que S é um semigrupo.)

(c) Defina $f: (S, *) \to (\mathbf{Q}, +)$ por meio de $f(a, b) = a/b$. Mostre que f é um homomorfismo.

(d) Encontre a relação de congruência $\sim$ em S determinada pelo homomorfismo f, isto é, $x \sim y$ se $f(x) = f(y)$

(e) Descreva $S/\sim$. $S/\sim$ possui um elemento identidade? Ele possui inversos?

B.49 Seja $S = \mathbf{N} \times \mathbf{N}$. Considere que $*$ é a operação em S definida por

$$(a, b) * (a', b') = (a + a', b + b')$$

(a) Encontre $(3, 4) * (1, 5)$ e $(2, 1) * (4, 7)$.

(b) Mostre que $*$ é associativa. (Logo, que S é um semigrupo.)

(c) Defina $f: (S, *) \to (\mathbf{Z}, +)$ por meio de $f(a, b) = a - b$. Mostre que f é um homomorfismo.

(d) Encontre a relação de congruência $\sim$ em S determinada pelo homomorfismo f

(e) Descreva $S/\sim$. $S/\sim$ possui um elemento identidade? Ele possui inversos?

Grupos

B.50 Considere $\mathbf{Z}_{20} = \{0, 1, 2, \ldots, 19\}$ sob adição módulo 20. Seja H um subgrupo gerado por 5 (a) Encontre os elementos e a ordem de H. (b) Encontre os co-conjuntos de H em $\mathbf{Z}_{20}$.

B.51 Considere $G = \{1, 5, 7, 11\}$ sob multiplicação módulo 12. (a) Encontre a ordem de cada elemento. (b) G é cíclico? (c) Encontre todos os subgrupos de G.

B.52 Considere $G = \{1, 5, 7, 11, 13, 17\}$ sob multiplicação módulo 18. (a) Construa a tabela de multiplicação de G (b) Encontre 5^{-1}, 7^{-1} e 17^{-1} (c) Encontre a ordem e o grupo gerado por: (i) 5, (ii) 13, (d) G é cíclico?

B.53 Considere o grupo simétrico S_4. Sejam $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ e $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

(a) Encontre $\alpha\beta$, $\beta\alpha$, α^2 e α^{-1} (b) Encontre as ordens de α, β e $\alpha\beta$

B.54 Prove os seguintes resultados para um grupo G.

(a) O elemento identidade e é único.

(b) Cada a em G possui um inverso único a^{-1}.

(c) $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$ e, de forma mais geral, $(a_1a_2 \ldots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1}a_1^{-1}$.

(d) $ab = ac$ implica $b = c$ e $ba = ca$ implica $b = c$.

(e) Para quaisquer inteiros r e s, temos $a^ra^s = a^{r+s}$, $(a^r)^s = a^{rs}$.

(f) G é abeliano se, e somente se, $(ab)^2 = a^2b^2$ para todo $a, b \in G$.

B.55 Seja H um subgrupo de G. Prove: (a) $H = Ha$ se, e somente se, $a \in H$. (b) $Ha = Hb$ se, e somente se $ab^{-1} \in H$. (c) $HH = H$.

B.56 Prove a Proposição B.5 Um subconjunto H de um grupo G é um subgrupo de G se (i) $e \in H$, (ii) para todo $a, b \in H$, temos $ab, a^{-1} \in H$.

B.57 Seja G um grupo. Prove:

(a) A interseção de qualquer número de subgrupos de G é também um subgrupo de G.

(b) Para qualquer $A \subseteq G$, $gp(A)$ é igual à interseção de todos os subgrupos de G contendo A

(c) A interseção de qualquer número de subgrupos normais de G é um subgrupo normal de G

B.58 Suponha que G é um grupo abeliano. Mostre que qualquer grupo fator G/H é também abeliano.

B.59 Suponha que $|G| = p$, onde p é um primo. Prove (a) G não possui subgrupos, exceto por G e $\{e\}$ (b) G é cíclico e todo elemento $a \neq e$ gera G

B.60 Mostre que $G = \{1, -1, i, -i\}$ é um grupo sob multiplicação, e mostre que $G \cong \mathbf{Z}_4$ ao darmos um isomorfismo explícito $f: G \to \mathbf{Z}_4$.

B.61 Seja H um subgrupo de G com apenas dois co-conjuntos à direita. Mostre que H é normal.

B.62 Seja $S = \mathbf{R}^2$ o plano cartesiano. Encontre o estabilizador H_a de $a = (1, 0)$ em S, onde G é o grupo a seguir agindo sobre S:

(a) $G = \mathbf{Z} \times \mathbf{Z}$ e G age sobre S por meio de $g(x, y) = (x + m, y + n)$ onde $g = (m, n)$. Isto é, cada elemento g em G é uma translação de S.

(b) $G = (\mathbf{R}, +)$ e G age sobre S por meio de $g(x, y) = (x\cos g - y\sin g, x\sin g + y\cos g)$. Isto é, cada elemento em G rotacional S sobre a origem em um ângulo g.

B.63 Seja S um polígono regular com n lados e G um grupo de simetrias de S.

(a) Encontre a ordem de G.

(b) Mostre que G é gerado por dois elementos a e b tal que $a^n = e$, $b^2 = e$ e $b^{-1}ab = a^{-1}$ (G é chamado de *grupo dihedral*.)

B.64 Suponha que um grupo G age sobre um conjunto S, digamos, por meio do homomorfismo $\psi \to \mathrm{PERM}(S)$.

(a) Prove que, para qualquer $s \in S$: (i) $e(s) = s$, (ii) $(gg')(s) = g(g'(s))$ onde $g, g' \in G$

(b) A órbita G_s de qualquer $s \in S$ é definida por $G_s = \{g(s) : g \in G\}$. Mostre que as órbitas formam uma partição de S.

(c) Mostre que $|G_s|$ = ao número de co-conjuntos do estabilizador H_s de s em G (Lembre-se de que $H_s = \{g \in G : g(s) = s\}$.)

B.65 Seja G um grupo abeliano e n um inteiro positivo fixo. Mostre que a função $f: G \to G$ definida por $f(a) = a^n$ é um homomorfismo.

B.66 Seja G um grupo multiplicativo de números complexos z tal que $|z| = 1$, e considere que $\mathbf{R}$ é um grupo aditivo de números reais. Prove $G \cong \mathbf{R}/\mathbf{Z}$.

B.67 Suponha que H e N são subgrupos de G com N normal. Mostre que: (a) HN é um subgrupo de G. (b) $H \cap N$ é um subgrupo normal de H (c) $H/(H \cap N) \cong HN/N$

B.68 Sejam H e K grupos. Considere que G é o conjunto produto $H \times K$ com a operação

$$(h, k) * (h', k') = (hh', kk').$$

(a) Mostre que G é um grupo (chamado de *produto direto* de H e K).

(b) Seja $H' = H \times \{e\}$. Mostre que: (i) $H' \cong H$, (ii) H' é um subgrupo normal de G, (iii) $G/H' \cong K$

Anéis

B.69 Considere o anel $\mathbf{Z}_{12} = \{0, 1, \ldots, 11\}$ de inteiros módulo 12. (a) Encontre as unidades de $\mathbf{Z}_{12}$. (b) Encontre as raízes de $f(x) = x^2 + 4x + 4$ sobre $\mathbf{Z}_{12}$. (c) Encontre os associados de 2.

B.70 Considere o anel $\mathbf{Z}_{30} = \{0, 1, \ldots, 29\}$ de inteiros módulo 30.

(a) Encontre -2, -7 e -11. (b) Encontre: 7^{-1}, 11^{-1} e 26^{-1}.

B.71 Mostre que, em um anel R: (a) $(-a)(-b) = ab$; (b) $(-1)(-1) = 1$, se R possuir um elemento identidade 1.

B.71 Suponha que $a^2 = a$ para todo $a \in R$. (Tal anel é chamado de anel *Booleano*.) Prove que R é comutativo.

B.73 Seja R um anel com um elemento identidade 1. Transformamos R em outro anel R' ao definirmos

$$a \oplus b = a + b + 1 \quad \text{e} \quad a * b = ab + a + b$$

(a) Verifique que R' é um anel. (b) Determine o elemento 0 e o elemento 1 de R'.

B.74 Seja G qualquer grupo abeliano (aditivo). Defina uma multiplicação em G por meio de $a * b = 0$ para todo $a, b \in G$. Mostre que isso transforma G em um anel.

B.75 Sejam J e K ideais em um anel R. Prove que $J + K$ e $J \cap K$ são também ideais.

B.76 Seja R um anel com unidade 1. Mostre que (a) $\{ra : r \in R\}$ é o menor ideal contendo a.

B.77 Mostre que R e $\{0\}$ são ideais de qualquer anel R.

B.78 Prove: (a) As unidades de um anel R formam um grupo sob multiplicação. (b) As unidades em $\mathbf{Z}_m$ são os inteiros que são relativamente primos a m.

B.79 Para qualquer inteiro positivo m, verifique se $m\mathbf{Z} = \{rm : r \in \mathbf{Z}\}$ é um anel. Mostre que $2\mathbf{Z}$ e $3\mathbf{Z}$ não são isomorfos.

B.80 Demonstre o Teorema B.10: Seja J um ideal em um anel R. Então os co-conjuntos $\{a + J \mid a \in R\}$ formam um anel sob as operações de co-conjuntos $(a + J) + (b + J) = a + b + J$ e $(a + J)(b + J) = ab + J$.

B.81 Demonstre o Teorema B.11: Seja $f: R \to R'$ um anel de homomorfismo com kernel K. Então K é um ideal em R e o anel quociente R/K é isomorfo a $f(R)$.

B.82 Seja J um ideal em um anel R. Considere o mapeamento (canônico) $f: R \to R/J$ definido por $f(a) = a + J$. Mostre que (a) f é um homomorfismo de anéis, (b) f é um mapeamento sobrejetor.

B.83 Suponha que J é um ideal em um anel R. Mostre que: (a) Se R é comutativo, então R/J é comutativo. (b) Se R possui um elemento identidade 1 e $1 \notin J$, então $1 + R$ é um elemento de unidade para R/J.

Domínios de integridade e corpos

B.84 Prove que se $x^2 = 1$ em um domínio de integridade D, então $x = -1$ ou $x = 1$.

B.85 Seja $R \neq \{0\}$ um anel comutativo finito com nenhum divisor zero. Mostre que R é um domínio de integridade, isto é, se R possui um elemento identidade 1.

B.86 Prove que $F = \{a + b\sqrt{2} \mid a, b \text{ racional}\}$ é um corpo.

B.87 Prove que $F = \{a + b\sqrt{2} \mid a, b \text{ inteiros}\}$ é um domínio de integridade, mas não um corpo.

B.88 Um número complexo $a + bi$, onde a e b são inteiros é chamado de *inteiro Gaussiano*. Mostre que o conjunto G de inteiros Gaussianos é um domínio de integridade. Além disso, mostre que as unidades são ± 1 e $\pm i$.

B.89 Sejam R um domínio de integridade e J um ideal em R. Prove que o anel fator R/J é um domínio de integridade se, e somente se, J é um ideal primo. (Um ideal J é *primo* se $J \neq R$ e se $ab \in J$ implica $a \in J$ ou $b \in J$.)

B.90 Seja R um anel comutativo com elemento unidade 1 e J um ideal em R. Prove que o anel fator R/J é um corpo se, e somente se, J é um ideal máximo. (Um ideal J é máximo se $J \neq R$ e nenhum ideal K está entre J e R, isto é, se $J \subseteq K \subset R$, então $J = K$ ou $K = R$.)

B.91 Seja D um anel de matrizes reais 2×2 na forma $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. Mostre que D é isomorfo ao corpo de complexos C, quando D é um corpo.

B.92 Mostre que o único ideal em um corpo K é $\{0\}$ ou K em si.

B.93 Suponha que $f: K \to K'$ é um homomorfismo de um corpo K em um corpo K'. Mostre que f é um *mergulho*, isto é, f é um para um. (Assumimos que $f(1) \neq 0$.)

B.94 Considere o domínio integral $D = \{a + b\sqrt{13},\ a, b \text{ inteiros}\}$ (Veja o Exemplo B.15(*b*).) Se $\alpha = a + \sqrt{13}$, definimos $N(\alpha) = a^2 - 13b^2$. Prove:

(i) $N(\alpha\beta) = N(\alpha)N(\beta)$.

(ii) α é uma unidade se, e somente se, $N(\alpha) = \pm 1$.

(iii) Entre as unidades de D estão ± 1, $18 \pm 5\sqrt{13}$; e $-18 \pm 5\sqrt{13}$.

(iv) Os números 2, $3 - \sqrt{13}$ e $-3 - \sqrt{13}$ são irredutíveis.

Polinômios sobre um corpo

B.95 Encontre as raízes de $f(t)$, assumindo que $f(t)$ possui uma raiz inteira. (a) $f(t) = t^3 - 2t^2 - 6t - 3$, (b) $f(t) = t^3 - t^2 - 11t - 10$; (c) $f(t) = t^3 + 2t^2 - 13t - 6$.

B.96 Encontre as raízes de $f(t)$, assumindo que $f(t)$ possui uma raiz racional. (a) $f(t) = 2t^3 - 3t^2 - 16t - 7$, (b) $f(t) = 2t^3 - t^2 - 9t + 9$

B.97 Encontre as raízes de $f(t) = t^4 - 5t^3 + 16t^2 - 9t - 13$, considerando que $t = 2 + 3i$ é uma raiz.

B.98 Encontre as raízes de $f(t) = t^4 - t^3 - 5t^2 + 12t - 10$, considerando que $t = 1 - i$ é uma raiz.

B.99 Para qualquer escalar $a \in K$, defina o *mapa de avaliação* $\psi_a : K[t] \to K$ por meio de $\psi_a(f(t)) = f(a)$. Mostre que ψ_a é um homomorfismo de anéis.

B.100 Prove: (a) Proposição B.14. (b) Teorema B.26.

Respostas dos Problemas Complementares

B.39 (a) 12, 15, 18 e 6; (b) sim, sim; (c) 1; (d) apenas 1 e ele é seu próprio inverso.

B.40 (a) 17, -32, 29/2; (b) sim, sim, (c) zero; (d) se $a \neq 1/2$, então a possui um inverso, que é $-a/(1 + 2a)$.

B.41 (a) Sim, (b) não; (c) não; (d) não faz sentido falarmos sobre inversos quando não existe um elemento identidade.

B.42 (a) Dezesseis, uma vez que existem duas escolhas, *a* ou *b*, para cada um dos quatro produtos *aa*, *ab*, *ba* e *bb*. (b) Seja $aa = b$, $ab = a$, $ba = b$ e $bb = a$. Então, $ab \neq ba$. Além disso, $(aa)b = bb = a$, mas $a(ab) = aa = b$.

B.43 (a) *A*, *D*; (b) nenhum.

B.44 (a) Sim; (b) sim, (c) sim; (d) não.

B.45 (a) $\{1, -1, 0\}$, (b) não existe um conjunto.

B.46 (a) Sim, sim, não, (b) sim, não, não.

B.47 (a) (3, 10), (−5, 1), (b) sim, não; (c) (1, 0), (d) o elemento (a, b) possui um inverso se $a \neq 0$, e seu inverso é $(1/a, -b/a)$.

B.48 (a) (19, 20), (18, 7). (d) $(a, b) \sim (c, d)$ se $ad = bc$. (e) $S/\sim$ é isomórfico aos números racionais positivos sob adição. Logo, $S/\sim$ não possui elementos identidade nem inversos.

B.49 (a) (4, 9), (6, 8); (d) $(a, b) \sim (c, d)$ se $a + d = b + c$. (e) $S/\sim$ é isomórfico a **Z**, uma vez que todo inteiro é a diferença de dois inteiros positivos. Logo, $S/\sim$ possui um elemento identidade, e tal elemento possui um inverso.

B.50 (a) $H = \{0, 5, 10, 15\}$ e $|H| = 4$. (b) H, $1 + H = \{1, 6, 11, 16\}$, $2 + H = \{2, 7, 12, 17\}$, $3 + H = \{3, 8, 13, 18\}$, $4 + H = \{4, 9, 14, 19\}$.

B.51 (a) $x^2 = 1$ se $x \neq 1$. (b) Não. (c) $\{1\}$, $\{1, 5\}$, $\{1, 7\}$, $\{1, 11\}$, G.

B.52 (a) Veja a Fig. B-9(*a*). (b) 11, 13 e 17; (c) (i) $|5| = 6$, $gp(5) = G$, (ii) $|13| = 3$, $gp(13) = \{1, 7, 13\}$. (d) sim, uma vez que $G = gp(5)$.

B.53 (a) Veja a Fig. B-9(*b*). (b) 4, 3 e 4.

×	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

(a)

$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ $\quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ $\quad \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

(b)

Figura B-9

B.60 $f(1) = 0, f(i) = 1, f(-1) = 2, f(-i) = 3$

B.62 (a) $\{(0, 0)\}$, (b) $\{2\pi r \mid r \in Z\}$.

B.69 (a) 1, 5, 7 e 11; (b) 4 e 10; (c) {2, 10}.

B.70 (a) 28, 23 e 19; (b) 13, 11; 26^{-1} não existe, uma vez que 26 não é uma unidade.

B.72 Mostre que $-a = a$ usando $a + a = (a + a)^2$. Em seguida, mostre que $ab = -ba$ por meio de $(a + b) = (a + b)^2$

B.73 (b) $-1 =$ elemento 0, $=$ elemento 1.

B.91 Mostre que f é um isomorfismo, onde $f\left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\right) = a + bi$.

B.93 *Sugestão:* Use o Problema B.92.

B.95 (a) $-1, (3 \pm \sqrt{21})/2$; (b) $-2, (3 \pm \sqrt{29})/2$; (c) $3, (-5 \pm \sqrt{17})/2$

B.96 (a) $-1/2, 1 \pm 2\sqrt{2}$, (b) $3/2, (-1 \pm \sqrt{13})/2$

B.97 $2 \pm 3i, (1 \pm \sqrt{5})/2$

B.98 $1 \pm i, (-1 \pm \sqrt{21})/2$

Índice